Санкт-Петербургский государственный университет

Чистякова Юлия Владимировна

Выпускная квалификационная работа

Преступления в сфере компьютерной информации: законодательная регламентация и квалификация

Уровень образования: бакалавр

Направление: Юриспруденция 40.03.01

Основная образовательная программа: Уголовное право ВМ.5788.2019

Научный руководитель:
Доцент кафедры уголовного права, кандидат юридических наук
Арзамасцев Максим Васильевич

Рецензент:
Клейменов Иван Михайлович
Ведущий советник Управления конституционных основ уголовной юстиции Секретариата Конституционного Суда РФ

Санкт-Петербург
2021 год

Оглавление

Введение

Правовая система государства, законодательные изменения, нормативно-правовая база напрямую зависят от развития науки, технического прогресса и глобальных перемен в жизни, к которым они ведут. Многие авторы отмечают, что арсенал предметов, методов, аналогий, фикций и презумпций права на сегодняшний день находится на пределе и требует инновационных, гибридных и актуальных решений[1].

Так, в связи с колоссальным развитием информационно-цифровой среды в целом, а значит и противоправных деяний в данной среде, уголовное право также претерпевает изменения и требует их. Постоянное развитие возможностей кибернетических технологий, динамика роста сети «Интернет», доступность и используемость компьютерных технологий предопределяют наличие повышенного интереса организованных преступных групп и отдельных лиц к использованию их в противоправных целях.

Впервые законодатель принял решение криминализовать такие новые формы уголовно-наказуемых деяний в 1996 году. Для этого в Уголовный Кодекс Российской Федерации была внесена глава 28 о преступлениях в сфере компьютерной информации, содержащая изначально лишь три статьи: ст. 272, ст. 273 и ст. 274. Ст. 274.1 была введена лишь в 2017 году Федеральным законом от 26 июля 2017 года № 194-ФЗ.

После введения главы 28, призванной защищать отношения, которые возникают в связи с противоправными посягательствами, затрагивающими сферу компьютерной информации, которая в свою очередь и является предметом в данной группе преступлений, законодатель стал редактировать те составы преступлений, в которых компьютерная информация является средством совершения преступлений. Так, законодателем были введены ст. 159.6 УК РФ о мошенничестве, совершенном в области компьютерной информации, ст. 171.2 о незаконной организации и проведении азартных игр,

[1] В.Н. Синюков. Фундаментальные проблемы юридической науки. Цифровое право и проблемы этапной трансформации российской правовой системы. МГЮА № 9 (154) Сентябрь 2019 года.

использующих информационно-коммуникационные сети, ч. 2 ст. 228.1 о сбыте наркотических средств, психотропных веществ или их аналогов, совершенных с использованием электронных или информационно-коммуникационных сетей и так далее. То есть, законодатель, понимая повышенную общественную опасность, латентность и лёгкость совершения такого рода преступлений внес ряд квалифицированных составов и специальных статей для более строгой квалификации таких преступлений.

Благодаря этому законодателем преследуется и частично достигается цель совершенствования уголовно-правового противодействия возникновению новых видов компьютерных преступлений. Тем не менее, в данной сфере на сегодняшний день существует ряд неразрешенных доктринальных и практических проблем. К таковым относится проблема правильного определения объекта преступлений главы 28, из которой следуют сложности квалификации при совершении многообъектных преступлений, одним или несколькими из которых являются преступления в сфере компьютерной информации; соотношение преступлений главы 28 с иными преступлениями, например, вымогательство, клевета, нарушение тайны личной переписки и т.д.; разновидности базовых преступлений в сфере компьютерной информации (например, DDoS-атаки) и рассмотрение квалификационных проблем на их примере; отсутствие единообразия и определенного подходе в правоприменительной практике. Данные проблемы мы попытаемся рассмотреть в нашей работе и предложить возможные варианты их решения.

1. Общая классификация преступлений главы 28 УК РФ

1.1. Объект преступления

Уголовная ответственность за преступления в сфере компьютерной информации предусмотрена главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ), которая включена в раздел IX УК РФ «Преступления против общественной безопасности и общественного порядка». В данный раздел также включены глава 24 «Преступления против общественной безопасности»; глава 25 «Преступления против здоровья населения и общественной нравственности»; глава 26 «Экологические преступления»; глава 27 «Преступления против безопасности движения и эксплуатации транспорта».

Глава 28 УК РФ состоит из четырех статей: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создания, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», ст. 274.1 «Неправомерной воздействие на критическую информационную инфраструктуру Российской Федерации».

Так, предлагаем в общем проанализировать элементы составов преступлений, предусмотренных главой 28 УК РФ.

Включение 28 главы в качестве структурного элемента в раздел IX УК РФ «Преступления против общественной безопасности и общественного порядка» позволяет в качестве общего объекта совокупность признать все общественные отношения, взятые под охрану уголовным законом. Данный тезис является наиболее определенным в части определения объекта преступлений в сфере компьютерной информации.

В целом вопрос об объекте преступлений в сфере компьютерной информации является спорным и точки зрения авторов по поводу определения объекта отличаются в отечественной литературе.

Тем не менее, говоря о родовом объекте, необходимо отметить, что на сегодняшний день вопрос с его определением является практически решенным. Однако, если обратиться к «правовой истории», то ранее учёные определяли объект преступления в сфере компьютерной информации по-разному. Так, Т.Г. Смирнова указывает, что «…родовым объектом данной группы преступлений является общественная безопасность»[2].

По мнению С.В. Бородина «включение статьи 272, как и статей 273 и 274 УК РФ, в раздел о преступлениях, посягающих на общественную безопасность и общественных порядок, определяет объект рассматриваемых преступлений»[3]. Данную позицию также в общем поддерживает В.С. Комиссаров, который считает, что, «поместив данную главу в раздел IX «Преступления против общественной безопасности и общественного порядка», Законодатель определил родовой объект посягательства преступлений в сфере компьютерной информации, как отношения общественной безопасности»[4].

Другие учёные полагают, что «… родовой объект компьютерных преступлений – общественная безопасность; видовым объектом преступлений в сфере компьютерной информации, позволившим выделить из в самостоятельную главу Кодекса, будет совокупность охраняемых уголовным законом интересов в области безопасности изготовления, использования и распространения компьютерной информации, информационных ресурсов, информационных систем и технологий»[5].

Анализируя разные позиции, М.Ю. Дворецкий приходит к выводу о том, что «с учётом места главы 28 в системе особенной части УК РФ можно сделать вывод о том, что законодатель относит преступления в сфере компьютерной информации к преступлениям против общественного порядка и общественной безопасности, а, следовательно, родовым (специальных» объектом

[2] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Автореф. … дис. канд. юрид. наук. М., 1998, С. 12.

[3] Комментарий к Уголовному Кодексу РФ/ Отв. ред. А.В. Наумов. М., 1996, с. 662.

[4] Уголовный кодекс РФ: постатейный комментарий/ Под ред. Н.Ф. Кузнецовой и Г.М. Миньковского. М., 1997, с. 581.

[5] Российское уголовное право. Особенная часть/ Под ред. В.Н. Кудрявцева и А.В. Наумова. М., 1997. С. 346.

преступлений в сфере компьютерной информации является общественная безопасность. … Мы полагаем, что видовым объектом преступлений в сфере компьютерной информации являются права и интересы личности, общества и государства по поводу использований ЭВМ, системы ЭВМ или сети ЭВМ»[6].

Продолжая говорить о родовом объекте преступления, необходимо изучить опыт зарубежных государств в части определения места рассматриваемой группы преступлений в уголовном законодательстве.

Начнём с государств, чьё законодательство и истории наиболее близки к Российской Федерации. Так, в УК Беларуси статьи об ответственности за компьютерные преступления находятся в главе 31 «Преступления против информационной безопасности». В УК Украины – в разделе XV1 «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей». В УК Республики Казахстан - в главе 7 «Преступления в сфере компьютерной информации». В УК Грузии – в главе XXXV «Компьютерные преступления». В УК Эстонской Республики – в главе 14 «Преступления в сфере компьютерной информации и обработки данных». В УК Азербайджанской Республики – в главе 30 «Преступления в сфере компьютерной безопасности». В УК Латвийской Республики – в главе XX «Преступные деяния против общественной безопасности и общественного порядка».

При этом на уровнях национального законодательства зарубежных стран наполнение терминов «информационная безопасность», «компьютерная информация», «компьютерные преступления» и т.д. не определено точно, что не позволяет дать точный анализ тому, насколько единообразен подход в расположении данной главы в системе уголовно-правовых норм. Тем не менее, необходимо признать, что некоторые государства идут по пути расширения объекта преступлений данной главы (как, например, в Латвийской Республике, где общим объектом является общественная безопасность и порядок, что

[6] Дворецкий М.Ю. Объект преступлений в сфере компьютерной информации: VI Державинские чтения, 2001, с. 25-26.

наиболее близко к Российской Федерации). Уголовный Кодекс Украины, наоборот, идёт по пути максимального сужения и называет общим объектом электронно-вычислительные машины, системы и компьютерную информацию. Данный подход наиболее далёк от российского. Что касается Беларуси, Казахстана, Грузии и Азербайджана, то объекты такого рода в данных государствах являют собой компиляцию терминов «информация», «безопасность», «компьютер», что представляется неким средним вариантом. Отдельно хотелось бы обратить внимание на эстонский вариант, в котором отдельно выделена обработка данных непосредственно в названии главы.

Необходимо также обратить внимание на то, что в доктрине, в том числе отечественной, существует большое количество терминов, которые часто употребляются, однако, не используются в УК РФ и иных нормативно-правовых актах, а, значит, и не имеют точных определений. Так, многие авторы отмечают, что такие термины как «компьютерные преступления», «информационные преступления», «компьютерная информация», «цифровые преступления», «киберпреступления» действительно не имеют сформированных значений, что является следствием отсутствия доктринальной позиции по отнесению конкретных противоправных деяний к преступлениям в данной сфере, так как информационные технологии постоянно развиваются и меняются. [7] Данная неопределенность связана с различными весьма противоречивыми позициями. Так, некоторые авторы полагают, что включение главы 28 в УК РФ ошибочно, поскольку данные преступления не являются самостоятельными составами или самостоятельной группой преступлений, а должны быть внесены в кодифицированную системы в виде особых составов или квалифицирующих признаков других преступлений[8]. Другие ученые полагают, что термин «компьютерные преступления» попросту не является

[7] Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств// Журнал прикладных исследований 2020 г. – 54 с.

[8] Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин – Москва: Юридическая литература, 1991. – 272 с.

уголовно-правовым, однако, широко употребляется в международно-правовой практике и активно используется в криминалистике и криминологии[9]. Существует группа ученых, выдвигавшая идею заменить термин «компьютерные преступления» на «информационные преступления»[10], которая, однако, была отклонена по причине того, что в случае использования термина «информационные преступления» выходит, что объектом такого преступления может выступать любая информация, хотя, разумеется, имеется в виду информация исключительно на машинных носителях. Мы полагаем, что на сегодняшний день нет необходимости в узаконивании всех вышеуказанных терминов, поскольку они все в какой-то части являются дублирующими и различаются лишь в небольших нюансах. Поэтому мы полагаем необходимым остановиться на уже законодательно закрепленном термине «преступления в сфере компьютерной информации». Он применяется также и на международном уровне, в том числе в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации. В нем указана следующая дефиниция: «Преступления в сфере компьютерной информации – уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация»11.

В отечественной доктрине также многие авторы предпринимали попытки дать определение используемому в том числе законодательно термину «преступления в сфере компьютерной информации». Так, И.Р. Бегишев под данными преступлениями понимает «предусмотренные уголовным законом виновно совершенные общественно опасные деяния, направленные на нарушение целостности, конфиденциальности, достоверности и доступности

[9] Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук; Сарат. юрид. ин-т МВД РФ – Саратов, 2002 г.

[10] Копылов В.А. Информационное право: вопросы теории и практики/ В.А. Копылов – Москва: Юристъ, 2003. – 623 с.

[11] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации - Исполнительный комитет СНГ.

охраняемой законом цифровой информации»12. В.А. Бессонов приводит следующее определение: «предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране имущественным правам и интересам, общественной и государственной безопасности и конституционному строю»13. Петрова И.А. и Лобачёв И.А. определяют такие преступления как «противоправное виновно совершенное общественно опасное деяние, наказуемое в уголовном порядке, посягающее на общественные отношения по безопасному производству, хранению, передаче, поиску, использованию, распространению или защите компьютерной информации, причинившее или создающее угрозу причинения вред охраняемым законом правам и интересам физических и (или) юридических лиц, общества, государства»14.

Анализируя вышеизложенные позиции, мы полагаем, что они не являются полностью совершенными по следующим причинам. Во-первых, все формулировки используют термины, не закрепленные законодательно, что порождает определенную путаницу. «Цифровая информация», «автоматизированные системы обработки данных», т.д. – все эти термины используются в доктрине, но не имеют законодательных дефиниций. Кроме того, данные определения наполнены большим количеством перечисляемых способов совершения преступления, которые не совпадают с перечнем, законодательно указанным в главе 28. Тем не менее, мы можем предпринять попытку сформулировать определение термину «преступление в сфере компьютерной информации». Мы полагаем, что преступление в сфере

[12] Бегишев И.Р. Цифровая информация: понятие и сущность как предмета преступления по российскому законодательству// Академический юридический журнал – 2011. 0 № 2 (44) с.10.

[13] Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук; Нижегородский юридич. Ин-т МВД РФ – Нижний Новгород, 2000.

[14] Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств// Журнал прикладных исследований 2020 г. – 59 с.

компьютерной информации – это предусмотренное уголовным законом виновно совершенное общественно опасное деяние, наказуемое в уголовном порядке, посягающее на отношения общественной безопасности и общественного порядка, права и интересы субъектов по обеспечению безопасности использования информации и информационных ресурсов и информационную безопасность в целом, а также компьютерную информацию.

Продолжая говорить о родовом объекте, также необходимо обратиться к опыту европейских государств в данном вопросе. Так, в Уголовном кодексе Франции глава «О посягательствах на системы автоматизированной обработки данных» расположена в книге 111 «О преступлениях против собственности»; в Уголовном кодексе ФРГ компьютерные преступления включены в раздел «Повреждение имущества», а в Уголовном кодексе Испании 1995 года статьи о компьютерных преступлениях вообще не выделены в отдельную главу.

Таким образом, можно сделать следующий вывод. В связи с неопределенностью большого количества используемых терминов, нельзя точно утверждать о наличии или отсутствии единообразия в понимании объекта преступления преступлений в сфере компьютерной информации. Однако, можно с уверенностью сказать, что законодатели всех государств отмечают, что характеристиками объекта являются то, что данная информация неотделима от машинного носителя, с ней можно производить ряд действий: она может создаваться, храниться, копироваться, использоваться, и данный список растет с развитием компьютерных технологий, объектом в том числе является такая информация, которая быстро обрабатывается, может быть уничтожена бесследно и передаются через информационно-телекоммуникационные каналы связи на любые расстояния.

При определении родового объекта необходимо также подчеркнуть, что преступления, предусмотренные главой 28 УК РФ, могут нанести вред не только отношениям, связанным с информационной безопасностью. Поскольку само содержание компьютерной информации может быть самым разнообразным, как и способы воздействия на неё в ходе совершения

преступления, последствиями компьютерных преступлений могут быть в том числе нарушение авторского права, разглашение сведений частной жизни, имущественный ущерб, сбои в системах управления транспортными средствами и спутниками, нарушение коммерческой тайны и даже смерть человека [15].

Так, как указывалось выше, на сегодняшний день практически не существует дискуссий по поводу определения родового объекта преступлений в сфере компьютерной информации. Доктрина ориентируется на юридико-техническое решение в виде помещения отдельной главы 28 в раздел «Преступления против общественной безопасности и общественного порядка». С учётом вышеизложенного, нам представляется верным определить родовой объект как отношения общественной безопасности и общественного порядка в целом, включающие в себя общественную безопасность, здоровье населения и общественную нравственность, экологическую безопасность, безопасность движения и эксплуатации транспорта.

Видовым объектом преступлений в уголовно-правовой доктрине признается совокупность тождественных общественных отношений одного вида, на которые посягает однородная группа преступлений. Что касается видового объекта, то в уголовно-правовой доктрине существуют различные точки зрения. Некоторые авторы определяют видовой объект как условия безопасности хранения и использования компьютерной информации[16]. Другие считают видовым объектом общественные отношения, обеспечивающие защищенность компьютерной информации от угрозы неправомерного доступа, распространения вредоносных программ и безопасность использования ЭВМ [17]. Третьи – совокупность общественных отношений по правомерному и безопасному использованию, хранению, распространению и защите

[15] Борисов Т. Хакеры остановили сердце. Преступность в Интернете дошла до физического устранения людей – прямо по проводам// Рос. газ. 2005. 8 февр.

[16] Уголовное право России. Части общая и особенная учебник/ отв. ред. А.И. Рарог – Москва, Проспект, 2016. – 494 стр.

17 Бобраков И.А. Уголовное право: учебник/ И.А. Бобраков – Саратов: Вузовское образования, 2018.

компьютерной информации, автоматизированных систем обработки информации, необходимых для нормальной жизнедеятельности общества в целом [18].

Анализируя позиции большинства авторов, как устаревших, так и современных[19], мы полагаем необходимым раскрыть понятие «видового объекта преступлений в сфере компьютерной информации» как группу общественных отношений, в которые включены права и интересы субъектов, по обеспечению безопасности использования информации и информационных ресурсов, необходимые для нормальной жизнедеятельности общества. Данную позицию также поддерживают А.В. Пелевина, Т.Г. Смирнова, И.А. Петрова и другие авторы[20]. Кроме того, некоторые авторы сокращают определение и отмечают, что видовым объектом является непосредственно информационная безопасность[21]. Этот же тезис отмечен и в работах авторов последних лет[22].

Далее необходимо проанализировать непосредственный объект исследуемой группы преступлений. Некоторые ученые считают, что непосредственным объектом преступлений являются общественные отношения, связанные с безопасностью информации [23]. Однако, с учетом того, что на сегодняшний день сложилось понимание насчет видового объекта, данное определение кажется несколько устаревшим. Другие полагают, что непосредственным объектом преступлений в сфере компьютерной информации

---

[18] Лопатина Т.М. Особенности объекта преступлений в сфере компьютерной информации: Бизнес в законе 1-2`2006, с. 171.

[19] Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств// Журнал прикладных исследований 2020 г. – 60 с.

20 Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Автореф. дисс. … канд. юрид. наук. – М., 1998, с. 12.

21 Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации. / Пробелы в российском законодательстве – 4`2015, с. 209.

22 Бимбинов А.А., Боженок С.А., Грачева Ю.В., Жевлаков Э.Н., Звечаровский И.Э., Иногамова-Хегай Л.В., Клепицкий И.А., Корнеева А.В., Кочои С.М., Левандовская М.Г., Новикова Е.В., Маликов С.В., Молчанов Д.М., Орешкина Т.Д., Палий В.В., Понятовская Т.Г., Рарог А.И., Рубцова А.С., Соктоев З.Б., Суспицына Т.П., Устинова Т.Д., Цепелев В.Ф., Чучаев А.И., Юрченко И.А. Уголовное право Российской Федерации. Особенная часть (учебник) (под ред. д.ю.н., проф. И.Э. Звечаровского). - М.: "Проспект", 2020. - 688 с.

[23] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. - № 10. – С. 25.

является часть информационных отношений, непосредственно связанных с операциями над компьютерной информацией[24]. Однако, мы полагаем, что для каждого состава преступления главы 28 УК РФ существует свой непосредственный объект. Данная позиция является господствующей на сегодняшний день и поддерживается многими авторами[25].

Так, А.В. Пелевина отмечает, что непосредственным объектом «выступают конкретные общественные отношения, которым преступление причиняет вред или создает угрозу его причинения». В том числе А.В. Пелевина отмечает складывающиеся в процессе обеспечения безопасности компьютерную информацию, правомерное безопасное использование телекоммуникационных сетей, конкретные права и интересы по поводу использования автоматизированных систем обработки данных; права владельца системы на неприкосновенность информации, установленный порядок правил эксплуатации системы [26]. Однако, более подробный анализ непосредственных объектов будет проведён нами в ходе анализа каждого состава преступления главы 28 УК РФ.

Также, в связи с тем, что, как отмечалось ранее, совершение преступлений, предусмотренных главой 28 УК РФ может нанести вред крайне разнообразным сферам общественных отношений, необходимо поставить вопрос об установлении дополнительных объектов преступлений. В случаях, когда в ходе совершения преступления происходит одновременное посягательство на две или более непосредственных объекта один из них будет основным, а другой – дополнительным, который в свою очередь будет либо причиной вменения квалифицированного состава, либо будет образовывать

[24] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Автореф. дисс. … канд. юрид. наук. – М., 1998, с. 12.

[25] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 1997. - № 1 – С. 9; Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность // Юридический мир. – 1998. - № 2. С. 350-352; Лопатина Т.М. Особенности объекта преступлений в сфере компьютерной информации: Бизнес в законе 1-2`2006, с. 171.

[26] Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации. / Пробелы в российском законодательстве – 4`2015, с. 209; Уголовное право. Особенная часть: учебник / под ред. проф. В.Н. Петрашова. М.: Издательство Приор, 1999. С. 364, 430.

идеальную совокупность и будет требовать дополнительной квалификации. Виды дополнительных объектов применительно к составам главы 28 УК РФ весьма разнообразны. Так, это могут быть конституционный строй и безопасность государства, личные имущественные и интеллектуальные права и интересы; конституционные права и свободы человека и гражданина; общественные отношения в сфере государственной власти; жизни и здоровья человека; мира и безопасности человечества. С данным тезисом согласны большинство авторов [27].

[27] Дворецкий М.Ю. Объект преступлений в сфере компьютерной информации: VI Державинские чтения, 2001, с. 26; Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации. / Пробелы в российском законодательстве – 4`2015, с. 210; Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации: учебно-практическое пособие, 2007. С. 127.

1.2. Предмет преступления

Что касается предмета данной группы преступлений, то необходимо отметить, что им, разумеется, не могут считаться сами материальные носители информации – ЭВМ, информационные структуры или информационные системы. Данные предметы являются предметами преступлений против собственности, регулируемых главой 21 УК РФ. Поэтому предметом преступлений главы 28 УК РФ вне всяких сомнений является компьютерная информация, что также подтверждается мнениями многих авторов [28]. Особенностью данной группы преступления является то, что именно компьютерная информация является в том числе и орудием или средством совершения преступления. В связи с ключевым значением данного термина для раскрытия признаков и особенностей преступления главы 28 УК РФ полагаем, что на определении и раскрытии понятия «компьютерная информация» необходимо остановиться подробнее.

Крылов В.В. в 1998 году раскрывает понятие компьютерной информации и поясняет, что «такая информация должна представлять документированную организованную форму, представляющую собой совокупность следующих элементов:

содержания информации;

реквизитов, позволяющих установить источник, полноту информации, степень её достоверности, принадлежность и другие параметры;

материального носителя информации, на котором её содержание и реквизиты закреплены»[29].

[28] Кузнецов А.П., Маршакова Н.Н., Паршин С,М. Преступления в сфере компьютерной информации: учебно-практическое пособие. Нижний Новгород, 2007. С. 184; Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации. / Пробелы в российском законодательстве – 4`2015, с. 210.

[29] Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского университета. Серия 11: Право. – 1998. - № 4. – С. 21.

На сегодняшний день, на наш взгляд, данное определение является несколько устаревшим, задаёт верный вектор для определения актуальных признаков компьютерной информации на сегодняшний день.

Так, в соответствии с разъяснением российского законодателя под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (см. п. 1 примечания к ст. 272 УК РФ). Определение термина «компьютерная информация» содержится также в Соглашении о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 01.06.2001), где обозначено, что компьютерная информация – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию электронно-вычислительных машин, или передающаяся по каналам связи. Соответственно, сегодня компьютерная информация может существовать в любом виде, но должна быть доступна восприятию электронно-вычислительных машин, из чего следует, что она должна быть представлена в форме электрических сигналов.

Актуальными общими криминалистическими признаками компьютерной информации являются[30]:

компьютерная информация является одной из объективных форм существования информации - электронной формой;

компьютерная информация всегда опосредована через электронный носитель информации, вне которого физически не может существовать;

доступ к компьютерной информации могут одновременно иметь несколько лиц;

[30] Метелев А.В., Образцов В.А., Поздняков В.М., Рычкалова Л.А., Селина Е.В., Степаненко Д.А., Табаков А.В., Тушканова О.В., Устинов А.В., Ширев Д.В., Шмонин А.В. Криминалистика: учебник для бакалавров (под ред. д.ю.н., проф. Л.В. Бертовского). - М.: "Проспект", 2018. - 960 с.

компьютерная информация достаточно просто и быстро преобразуется из неэлектронных форм в электронную и обратно, например, при сканировании документа с бумажного носителя и последующей распечатки на бумаге его электронного образа;

компьютерная информация копируется на различные виды электронных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;

компьютерная информация собирается, исследуется и используется в целях уголовного судопроизводства только с помощью специальных научно-технических средств - средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей (компьютерных программ, баз данных, информационных систем, электронных носителей информации и т.д.).

Существует несколько классификаций компьютерной информации [31].

Так, по юридическому положению компьютерная информация может быть документированной или недокументированной. Документированная компьютерная информация - это зафиксированная на электронном носителе путем документирования информация с электронными реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. Недокументированная компьютерная информация - это данные, управляющие команды и сигналы, образующиеся и (или) используемые в процессе обработки информации и не обладающие признаками документа, например, логин и пароль доступа к сети Интернет или ее ресурсу, сетевой адрес, доменное имя, ключ электронной подписи. Классификация по данному признаку позволяет отметить динамику изменений понятия компьютерной информации, ведь,

[31] Метелев А.В., Образцов В.А., Поздняков В.М., Рычкалова Л.А., Селина Е.В., Степаненко Д.А., Табаков А.В., Тушканова О.В., Устинов А.В., Ширев Д.В., Шмонин А.В. Криминалистика: учебник для бакалавров (под ред. д.ю.н., проф. Л.В. Бертовского). - М.: "Проспект", 2018. - 452 с.

например, в соответствии с классификацией Крылова В.В. компьютерная информация должна была иметь только документированную форму.

По режиму уголовно-правовой охраны компьютерная информация может быть общедоступной или охраняемой законом. Понятие охраняемой законом компьютерной информации можно раскрыть с помощью смежного законодательства. Так, это сведения, отнесенные законодательством Российской Федерации к различным видам тайн (государственной, служебной, коммерческой, банковской, связи и др.), а также персональные данные, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

По форме представления компьютерная информация может относиться к следующим видам: сетевой адрес, доменное имя, файл, электронная подпись, электронное сообщение, электронный документ, компьютерная программа, база данных, информационная система, сайт, страница сайта.

Сетевой адрес – это идентификатор в сети передачи данных или иные средства связи, входящие в информационную систему.

Доменное имя – это набор символов, предназначенный для адресации сайтов в информационно-телекоммуникационной сети.

Файл – это поименованная область записей на электронном носителе информации, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать.

Электронная подпись – это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронный документ – это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия

человеком с использованием ЭВМ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Компьютерная программа – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

База данных – это представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ.

Сайт – это совокупность программ для ЭВМ и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в информационно-телекоммуникационной сети.

Страница сайте – это часть сайта в информационно-телекоммуникационной сети, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта.

Таким образом, предмет преступлений главы 28 УК РФ довольно разнообразен и охватывает все возможные формы и виды информации, представленной в электронном виде. Также можно сделать вывод, что с течением времени количество видов предметов увеличивается, ведь сфера компьютерных технологий не стоит на месте и развивается крайне активно.

1.3. Объективная сторона преступления

Говоря о следующем элементе, а именно – об объективной стороне, нужно отметить следующее. Деяния, составляющие объективную сторону преступлений данной главы, совершаются в форме действия, за исключением преступлений, предусмотренных ст. 274 и ч. 3 ст. 274.1 УК, совершение которых возможно и бездействием. Четыре из шести основных составов преступления (ч. 1 ст. 272, ч. 1 ст. 274, ч. 2 и 3 ст. 274.1 УК) сконструированы как материальные. В ч. 1 ст. 273 и ч. 1 ст. 274.1 УК содержатся формальные составы преступлений.

Для анализа следующих признаков необходимо отметить следующее. В связи с тем, что сфера компьютерных преступлений является весьма специфической и требующей специальных познаний, большинство норм сформулированы по принципу бланкетных. Поэтому для установления всех признаков объективной стороны требуется анализ большого объёма смежных нормативно-правовых актов.

Так, говоря о месте совершения преступления, нужно сказать, что при выявлении и расследовании преступлений в сфере компьютерной информации установление конкретного места совершения преступления часто вызывает большую сложность. Нередко место непосредственного совершения противоправного деяния географически не совпадает с местом наступления общественно опасных последствий. Поэтому для данной группы преступлений выделяют несколько мест: место обнаружения признаков преступления; место непосредственного совершения преступных деяний; место подготовки (приискания) средств совершения преступления. Данные места могут физически находиться не рядом, могут быть удалены друг от друга даже в масштабе разных стран. Это связано с тем, что компьютерные преступления совершаются посредством дистанционного доступа к компьютерной информации, подвергающейся преступному воздействию, и с использованием мобильных современных средств цифровой связи. Поэтому, в соответствии с судебной практикой и

позицией большинства авторов местом совершения преступления считают то транспортное средство, участок местности или территорию помещения, учреждения, предприятия, организации, государства, где были совершены общественно опасные деяния, независимо от места наступления преступных последствий. Так, в качестве наиболее типичных мест совершения такого рода преступлений можно привести жилище преступника (около половины случаев); место его работы (учебы), не являющееся местом нахождения потерпевшего (в каждом третьем случае); общественное место, являющееся местом установки стационарного или подключения мобильного компьютерного терминала - средства совершения преступления; по месту нахождения потерпевшего совершается [32].

Что касается времени совершения преступления, то необходимо отметить, что общественно опасные последствия могут быть отсрочены по времени (например, создание и внедрение вредоносной программы может быть совершено значительно раньше, чем наступят общественно опасные последствия в виде утечки информации). Тем не менее, временем совершения преступления признается время окончания общественно опасного деяния независимо от времени наступления последствий. В связи со спецификой совершения преступлений данное время возможно установить с точностью до минут и секунд, поскольку ЭВМ производят автоматическую регистрацию наиболее значимых операций и фиксируют события, связанные с обработкой компьютерной информации [33].

Способов совершения преступлений, предусмотренных главой 28 УК РФ, крайне много и привести исчерпывающий список не представляется возможных. Однако, исходя из проанализированной судебной практики и изученной литературы, можно выделить следующие наиболее часто

32 Метелев А.В., Образцов В.А., Поздняков В.М., Рычкалова Л.А., Селина Е.В., Степаненко Д.А., Табаков А.В., Тушканова О.В., Устинов А.В., Ширев Д.В., Шмонин А.В. Криминалистика: учебник для бакалавров (под ред. д.ю.н., проф. Л.В. Бертовского). - М.: "Проспект", 2018. - 960 с.

33 Вехов В.Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. N 4. С. 2-4.

используемые способы: хищение электронных носителей информации; неправомерный доступ к электронным носителям информации; неправомерный доступ к охраняемой законом компьютерной информации; неправомерное копирование охраняемой законом компьютерной информации; неправомерный доступ к информационно-телекоммуникационной сети; создание вредоносных компьютерных программ; использование вредоносных компьютерных программ; распространение вредоносных компьютерных программ с использованием информационно-телекоммуникационной сети и (или) электронного носителя информации; внесение изменений в существующие программы; дезактивация либо обход средства защиты компьютерной информации; перехват компьютерной информации из канала электросвязи; уничтожение, блокирование либо копирование компьютерной информации с использованием специально приспособленных, разработанных, запрограммированных технических средств для негласного получения информации; нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования[34].

34 Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. М.: Академия Следственного комитета Российской Федерации. 2015. N 2. С. 43-46.

1.4. Субъект преступления

Субъектом преступления в сфере компьютерной информации по общему правилу является физическое вменяемое лицо, достигшее возраста, установленного ст. 19 УК РФ, а именно – 16 лет. В некоторых составах (ч. 3 ст. 272, ч. 2 ст. 273, ст. 274 и ч. 3 ст. 274.1) речь идет о специальном субъекте, обладающим особыми признаками. Например, лицо, использующее своё служебное положение, лицо, имеющее доступ к средствам хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационным сетям.

Описывая субъект данного преступления с криминалистической точки зрения, необходимо отметить, что данные лица обладают высокой степенью общественной опасности. Они интеллектуально развиты, являются профессионалами в своей сфере, крайне скрытны, в связи с чем многие такого рода преступления остаются латентными, обладают большим объёмом специальных знаний и практических навыков в сфере компьютерных технологий. Часто это сотрудники учреждений и предприятий, использующих компьютерные технологии в своей административно-хозяйственной деятельности. Исходя из судебной практики большинство преступников в данной области являются мужчинами в возрасте до 30 лет. Данные лица почти никогда не являются рецидивистами, особенно в части совершения других преступлений.

1.5. Субъективная сторона преступления

По содержанию субъективной стороны большая часть преступлений - умышленные (ст. 273, ч. 1 ст. 274.1 УК). Статья 274 и ч. 3 ст. 274.1 УК предусматривают ответственность за неосторожные преступления. Часть преступлений может быть совершена как по неосторожности, так и умышленно (ст. 272, ч. 2, 4, 5 ст. 274.1 УК). Мотивы и цели преступлений, предусмотренных главой 28 УК РФ, являются факультативными признаками и не влияют на квалификацию. Исходя из судебной практики, мотивы и цели совершения преступления могут быть следующими: корысть, стремление скрыть другое преступление, хулиганские побуждения и озорство, демонстрация личных интеллектуальных способностей или превосходства, месть, исследовательские цели[35].

[35] Метелев А.В., Образцов В.А., Поздняков В.М., Рычкалова Л.А., Селина Е.В., Степаненко Д.А., Табаков А.В., Тушканова О.В., Устинов А.В., Ширев Д.В., Шмонин А.В. Криминалистика: учебник для бакалавров (под ред. д.ю.н., проф. Л.В. Бертовского). - М.: "Проспект", 2018. - 354 с.

2. Проблемы и особенности преступлений в сфере компьютерной информации

2.1. Разграничение составов преступлений главы 28 УК РФ и мошенничества в сфере компьютерной информации

Преступление, предусмотренное ст. 159.6 УК РФ, а именно мошенничество в сфере компьютерной информации, отличается от остальных видов мошенничества в первую очередь способ совершения преступления. В соответствии с п. 20 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – постановление Пленума ВС РФ № 48) он определяется как целенаправленное воздействие программных или программно-аппаратных средств на серверы, средства вычислительной техники, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. Таким образом, встаёт вопрос о разграничении составов преступления главы 28 УК РФ и данного специального вида мошенничества.

Полагаем необходимым начать с двух тезисов. Во-первых, Верховный Суд РФ даёт определенные разъяснения на этот счет в п. 20 Постановления Пленума от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором указано, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ. Тем не менее, данная рекомендация подвергается большому сомнению в научном сообществе, что мы обсудим ниже.

Во-вторых, для решения о наличии или отсутствии совокупности мы полагаем необходимым определить, является ли преступление,

предусмотренное ст. 159.6 многообъектным или нет, поскольку если мошенничество в сфере компьютерной информации имеет своим объектом только отношения собственности, то необходимость квалификации по совокупности существенно возрастает. Напротив, если мошенничество в сфере компьютерной информации охватывает причинение вреда как отношениям собственности, так и информационной безопасности, то в данной ситуации остро встаёт вопрос о нарушении принципа недопустимости двойного вменения при квалификации по совокупности.

Так, по мнению Е.Н. Бархатовой, мошенничество в сфере компьютерной информации имеет два предмета: компьютерную информацию и имущество[36]. Однако, в этой же статье Е.Н. Бархатова пишет о том, что «именно компьютерная информация, зачастую не являясь предметом посягательства, представляет собой обязательный элемент способа его совершения». Данное противоречие вызывает неоднозначность в позиции автора, однако, наталкивает на вывод о том, что всё-таки преступление, предусмотренное ст. 159.6 УК РФ нельзя считать многообъектным. При этом нельзя отрицать, что компьютерная информация (или информационная безопасность) тем не менее являются элементом состава данного преступления. Мы считаем, что компьютерная информация выполняет роль элемента не объекта, а объективная стороны, а именно средства совершения преступления. Такой же позиции придерживается Н.А. Лопашенко[37] в своих исследованиях.

Таким образом, с учетом того, что явного пересечения в объекте преступлений главы 28 и мошенничества в сфере компьютерной информации не имеется, можно сделать вывод о допустимости двойной квалификации и проанализировать проблемы совокупности с каждым из составов.

Авторы, исследовавшие данный вопрос приходят к противоречивым выводам. Там, С.Я. Бойко указывает, что мошенничество в сфере

[36] Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. № 9.
[37] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Уголовное право и процесс. 2020. VI.

компьютерной информации необходимо отличать от посягательств против компьютерной безопасности, однако, не предлагает критериев и не выдвигает варианты квалификаций. [38]

З.И. Хисамова говорит о том, что норма статьи 159.6 УК РФ является специальной по отношению к нормам ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ [39].

При этом М.И. Третьяк, напротив, считает, что соотношения как части и целого между деяниями, предусмотренными в ст. 159.6 и ст. 272 и 273 не имеется [40].

Таким образом, единообразия в подходе при разрешении данной квалификационной проблемы на сегодняшний день не имеется.

Необходимо отметить, что при попытке предложить верный вариант квалификации, мы столкнулись с несколькими проблемами. Во-первых, основной проблемой является то, что в ст. 159.6 УК РФ и в преступлениях главы 28 законодателем употребляются лишь частично пересекающиеся понятия. Трудно предположить, была ли в этом задумка законодателя, либо вышло ли это не нарочно. Однако, в диспозиции ст. 159.6 УК РФ законодателем указаны следующие признаки: *ввод, удаление, блокирование, модификация либо иное вмешательство.* При этом п. 20 Постановления Пленума Верховного Суда от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняет, что вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается *целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или*

[38] Бойко С.Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование. М.: Юрлитинформ, 2019. – 198 с.

[39] Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1. С. 118.

[40] Третьяк М.И. Мошенничество как преступление против собственности в современном уголовном праве: курс лекций. М.: Юрлитинформ, 2014 – 198 С.

на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. То есть, Верховный Суд оставляет понятие «вмешательство» довольно открытым и неисчерпывающим, что в итоге делает перечень способов совершения деяние в ст. 159.6 казуально-абстрактным[41].

При этом в главе 28 законодатель использует лишь четыре понятия: *уничтожение, блокирование, модификацию и копирование.*

Соответственно, в ст. 159.6 и главе 28 есть полное совпадение по признакам «блокирование» и «модификация», смысловое совпадение по признаку «удаление»/ «уничтожение» и различия по признакам «копирование» (который имеется в главе 28) и «ввод» (который имеется в ст. 159.6).

Тут необходимо отметить, что указанные выше признаки в сравниваемых составах выполняют разную роль. Так, в ст. 159.6 указанные признаки выполняют роль альтернативных способов совершения деяния. При этом в ч. 1 ст. 272 и ч. 1 ст. 274 они выполняют роль опасных последствий, а в ч.1 ст. 273 и ч. 1 ст. 274.1 УК РФ – двойную роль преступной цели и альтернативного последствия, хотя некоторые авторы считают, что данный признак выполняет роль функционально-целевой характеристики преступного средства[42]. Во-вторых, необходимо сказать о сходстве терминов «уничтожение» и «удаление». Всё указывает на их тождество, однако, основным нюансом может быть потенциальная возможность восстановления утраченной информации, что и может быть критерием различия данных терминов. Однако, в соответствии с Методическими рекомендациями по осуществление прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации уничтожение информации – это приведение информации или ее

[41] Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий // Вопросы российской юстиции. Четвертый выпуск. – 447 с.

[42] Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий // Вопросы российской юстиции. Четвертый выпуск. – 447 с.

части в непригодное для использования состояние *независимо от возможности ее восстановления.* Разъяснения термина «удаление», который используется в ст. 159.6, в нормативно-правовой базе не имеется. Однако, в связи с тем, что есть чёткое определения уничтожения, которое говорит о том, что возможность восстановления информации не имеет значения, можно с уверенностью сказать, что термины «уничтожение» и «удаление» как минимум соотносятся как целое (в котором возможность восстановления не имеет значения) и частное (в котором возможность восстановления теоретически имеет значение). Соответственно, можно сделать вывод о взаимозаменямости и условном тождестве данных терминов. В-третьих, что касается термина «ввод», который употребляется в ст. 159.6 и не употребляется в главе 28, то необходимо отметить, что данный признак в принципе не является самостоятельным. Неправомерный ввод информации так или иначе повлечет её модификацию, а значит, что операция «ввод» является частью операции «модификация». В-четвёртых, поскольку, как отмечалось выше, в ст. 159.6 перечень способ совершения преступления является открытым, на самом деле исключает препятствия для рассмотрения последствия ст. 272 «копирования» одновременно как способ совершения для 159.6 в виде копирования, что также нивелирует терминологическую разницу при формулировке диспозиций составов. Некоторые авторы, однако, отмечают, что похищение путём копирования невозможно[43], однако, для нас данная позиция не является однозначной.

Соответственно, на первый взгляд кажется, что вышеизложенные признаки являются дублирующими, что указывает на их сходство и подвергает большому сомнению возможность квалификации по совокупности. Однако позиция Верховного Суда РФ однозначна – возможные причины этого мы разберем ниже. Тем не менее, в защиту позиции Верховного Суда РФ мы хотим отметить, что данные признаки в разных составах играют разную уголовно-

[43] Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий // Вопросы российской юстиции. Четвертый выпуск. – 447 с.

правовую роль. Так, например, при убийстве, совершенном с использованием оружия, на которое у лица не имеется лицензии, мы будем квалифицировать содеянное по совокупности ст. 105 и ст. 222, хотя огнестрельное оружие является одновременно элементом обоих составов: в убийстве – средство совершения преступления, в ст. 222 – предмет преступления. Таким образом, двойного вменения не происходит, хотя вменяются два состава по одному и тому же признаку, являющемуся разным элементом каждого состава преступления. Полагаем, что данная логика применима и в анализируемой ситуации в части вменения ст. 159.6 и преступления главы 28 по совокупности.

Также необходимо отметить следующее. Криминообразующим признаком преступлений некоторых составов преступлений главы 28, в частности, ст. 272, вопрос о совокупности с который является самым спорным, является неправомерность. В соответствии с Методическими рекомендациями по осуществление прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации неправомерный доступ - это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее). При этом ст. 159.6 не анализирует вопрос правомерности доступа в принципе. Из этого следует, что в случае совершения мошенничества по ст. 159.6, когда доступ к информации был правомерным, возможность дополнительного вменения ст. 272 исключается в принципе. Некоторые авторы полагают, что данный вывод противоречит Постановлению Пленума № 48, однако, мы с этим не согласны44. В п. 20 Верховный Суд указывает, что квалификация по совокупности со ст. 272, 273 и 274.1 требуется только в случае

[44] Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий // Вопросы российской юстиции. Четвертый выпуск. – 446 с.

мошенничества в сфере компьютерной информации, *совершенного посредством неправомерного доступа* к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ.

Так, проанализируем каждый состав.

Говоря о ст. 274.1 мнение всех авторов[45] единогласно совпадает с позиций Верховного суда. Непосредственным объектом состава преступления, предусмотренного ст. 274.1 является критическая информационная инфраструктура РФ. В соответствии с п. 6 ст. 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» критическая информационная инфраструктура – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. При этом объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. В свою очередь субъектами критической информационной инфраструктуры являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели,

[45] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Уголовное право и процесс. 2020. VI.

которые обеспечивают взаимодействие указанных систем или сетей. Таким образом, поскольку ст. 274.1 предусмотрена охрана особого объекта, не являющегося элементом преступления ст. 159.6, дополнительная квалификация необходима всегда.

Говоря о ст. 273, необходимо отметить следующее. В ст. 273 УК уничтожение, блокирование, модификация компьютерной информации выступают целью создания, распространения или использования компьютерных программ либо иной компьютерной информации – вредоносных программ. Кроме того, состав преступления в ст. 273 является формальным и не требует наступления общественно-опасных последствий для его вменения. Соответственно, объективная сторона ст. 273 будет предшествовать совершению объективной стороны ст. 159.6. Таким образом, момент окончания преступления, предусмотренного ст. 273, предопределяет необходимость совокупной квалификации. Кроме того, с учетом того, что мошенничество является формой хищения, обязательным признаком которого является корыстность, по совокупности необходимо вменять ч. 2 ст. 273. Такой вывод подтверждается в том числе судебной практикой[46].

Ситуация со ст. 272 и ст. 274 сложнее. Так, большинство авторов склоняются к тому, что вменение по совокупности не является верным решением. Так, Лопашенко Н.А. полагает, что наличие дублирующих признаков в ст. 272 (уничтожение/удаление, блокирование, модификация) позволяет сделать вывод, что состав неправомерного доступа всегда полностью выполняется в компьютерном мошенничестве и является его частью. Такой же вывод делает Лопашенко Н.А. относительно ст. 274, о которой не упоминается в Постановлении Пленума Верховного Суда № 48. Таким образом, он делает вывод о том, что дополнительная квалификация компьютерного мошенничества по ст. ст. 272 и 274 УК не требуется[47]. При этом данный автор

46 Приговор № 1-588/2018 от 9 ноября 2018 г. по делу № 1-588/2018

47 Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Уголовное право и процесс. 2020. VI.

делает оговорку, что такой вывод следует лишь на первый взгляд и если не учитывать вопрос о санкций в данных статьях.

При этом данный вопрос является чуть ли не предопределяющим в решении данной проблемы. Так, получается, что составы компьютерных преступлений караются иногда жестче, чем состав компьютерного мошенничества. Максимальная санкция ч. 1 ст. 159.6 – арест на срок до 4 месяцев. При этом максимальная санкция ч. 1 ст. 272 и ч. 1 ст. 274 – лишение свободы на срок до 2 лет. Такие санкции порождают большое количество проблем. Выходит, что если мы избегаем квалификации по совокупности, то если лицо лишь нарушит правила эксплуатации или воспользуется неправомерным доступом к информации, повлекшим указанные последствия, то его максимальная санкция существенно строже, чем если он потом ещё совершит мошенничество. Таким образом, чтобы лицо получило меньшее наказание, ему необходимо совершить большее преступление.

С учетом этого решения законодателя в части назначения санкций двух данных статей, Лопашенко Н.А. приходит к выводу о необходимости квалификации по совокупности, однако, считают данный вариант квалификации принципиально неверным, поскольку отмечает, что если признаки одного преступления полностью входят в число признаков другого преступления, предусматривающего и дополнительные признаки, должен применяться только последний состав, из чего следует вывод, что в чистом виде ст. 272 (274) и 159.6 конкурируют как часть и целое.

К схожему выводу приходит Савельев И.В., который, отмечает, что Верховный Суд старается преодолеть созданный законодателем перекос в части более строго наказания, а законодатель заставляет правоприменителя выбирать либо общие конституционный веления, касающиеся охраны отношений и потерпевших и реализации задач уголовного закона, либо принцип справедливости и принципа толкования неустранимых сомнений в пользу виновного.

Тем не менее, мы не можем согласиться с данными выводами. Как указывалось выше, мы считаем, что ст. 159.6 и преступления главы 28 не соотносятся как часть и целое и не дублируют друг друга. В данных составах имеются одинаковые признаки, которые, как, кстати, отмечали оба автора, выполняют разные уголовно-правовые роли в составах данных преступлений. Поэтому данные составы с материальной точки зрения не противоречат правилам назначения наказания по совокупности. Учитывая данное обстоятельство, выбор законодателем санкций также не являет собой проблемы, поскольку даже без учета указанных санкций данные составы должны назначаться по совокупности.

Тем не менее, мы усматриваем иные проблемы в данной ситуации. Во-первых, не совсем понятно решение Верховного Суда относительно ст. 274. Почему Верховный Суд исключает возможность вменения данного состава по совокупности со ст. 159.6? Некоторые авторы выдвигают версии о том, что это связано с тем, что Верховный Суд расценивает ст. 274 как неосторожный состав. Однако, мы полагаем, что поводов так считать не имеется, поскольку в ст. 274 не сказано о том, что данный состав является неосторожным и он ничем не отличается с точки зрения конструкции от ст. 272. Соответственно, решение Верховного Суда РФ в данном вопросе остается непонятным и можно лишь ожидать разъяснений на этот счет, ведь на самом деле проблема дополнительной квалификации по ст. 274 также стоит достаточно остро.

Во-вторых, в таком случае получается, что состав преступления 159.6 крайне несамостоятельный. Не усматривается ситуации, при которой он мог бы вменяться сам по себе, без вменения состава из главы 28. Данное обстоятельство однозначно свидетельствует о несовершенной юридической технике законодателя и ущемляет права осужденных. Мы считаем, что данная проблема является критической и требует решения со стороны законодателя. Мы полагаем, что данная проблема может быть решена несколькими способами. Во-первых, не лишено смысла исключение статьи 159.6 из УК РФ в целом и внести изменения в состав мошенничества квалифицирующий признак

в виде «путём уничтожения, блокирования, модификации или копирования компьютерной информации». Таким образом, мы добиваемся терминологического единообразия в части соответствия главы 21 главе 28. Также в таком случае полностью исключаются споры относительно дублирующих признаков, поскольку из конструкции статьи следует, что данный состав будет являться специальным по отношению к ст. 159, а компьютерная информация однозначно будет выражена в виде средства совершения преступления. При такой редакции всегда будет необходима квалификация по совокупности, поэтому соотношения санкций ст. 159.6 и статей главы 28 не будет иметь решающего значения. Минусом такого варианта является то, что данный квалифицированный состав всё равно не будет работать самостоятельно и всегда будет требовать квалификации по совокупности. Тем не менее, возможен другой, обратный вариант, когда составу ст. 159.6 придаются черты специального состава по отношению к статьям главы 28. В таком случае необходимо сформулировать данную статью таким образом, чтобы было очевидно предназначение «компьютерной информации» как дополнительного объекта преступления. Кроме того, необходимо, чтобы в ст. 159.6 присутствовали квалифицирующие признаки, «перекрывающие» все составы главы 28, в том числе ст. 273 и ст. 274.1 При этом необходимо, чтобы санкция такого специального и, разумеется, квалифицированного и по отношению к главе 21, и по отношению к главе 28, была выше и чем в простом составе мошенничества, и чем в простых составах главы 28. Таким образом, мы очевидно демонстрируем соотношение статей главы 28 и ст. 159.6 как общих и специальной, что исключает возможность квалификации по совокупности, делает каждый из составов применимым по отдельности и полностью соответствует принципу недопустимости двойного вменения.

2.2. Проблемы квалификации преступлений, предусмотренных главой 28, на примере DDoS-атак

DDoS, сокращенно от Distributes Denial of Service (Распределенный отказ от обслуживания), это один из видов сетевой атаки, так называемый интернет-рэкет. Действие такого механизма основывается на том, что любые сетевые ресурсы (речь о веб-серверах) не безграничны. Все они имеют ограничения по количеству запросов, которые они могут одновременно обслуживать. И действие DDos-атаки заключается в искусственном увеличении одновременных запросов на сетевой ресурс, следствием чего может являться либо существенное замедление времени ответа за запросы, либо полный отказ в обслуживании всех запросов пользователей.

Например, один из известных веб-серверов Apache может одновременно выдерживать 255 конечных соединений. Проще говоря, одновременно на сайт, который хранится на данном сервере, могут зайти 255 пользователей. При использовании DDoS-атаки на данный сайт автоматически и искусственно отправляется более 255 запросов, на которые этот сайт рассчитан. И тогда реальные пользователи, которые хотят воспользоваться данным сайтом, попросту не смогут этого сделать, так как веб-сервер из-за перегруженности искусственными запросами вследствие DDoS-атаки не сможет передать им данные сайта.

Каким же образом осуществляется DDoS-атака? Это наиболее интересный с квалификационной точки зрения вопрос. Главный вопрос заключается в том, откуда именно возникают эти автоматические и искусственные запросы и как ими управлять. Для этого киберпреступник создает сеть из зараженных «зомби-компьютеров», принадлежащих третьим лицам. Такая сеть обычно называется «ботнет» (сеть ботов, роботов). Для создания ботнета киберпреступник использует специальную троянскую программу, так называемый Trojan-clicker (интернет-кликер). Функцией такой программы является организация несанкционированных обращений к интернет

ресурсам, в частности, к веб-страницам. Интернет-кликер зачастую является так называемым сетевым червём, то есть проникает в компьютер третьего пользователя практически любым возможным путем: скачивание файла любого формата, программы, перехода по ссылке и т.д. Для организации массовых DDoS-атак киберпреступник может заражать сотни тысяч компьютеров, при этом пользователи данных компьютеров не будут знать ни о наличии такой вредоносной программы на своем компьютере, ни о том, как и зачем она функционирует, а киберпреступник сможет активировать и деактивировать данную программу в любой нужный для него момент.

Примером физической, реальной «DDoS-атаки» может являться история одного супермаркета в Новосибирске, в котором были введены правила об отказе в обслуживании покупателей, которые не взяли корзинку или тележку. Люди были возмущены таким правилом и устроили флешмоб: несколько сотен человек пришли в этот супермаркет, взяли тележки, и каждый из них купил лишь один творожный сырок, а затем встали в очередь к кассам. Из-за такого массового нашествия на магазин, работа в нем была парализована, и он потерпел существенные убытки. Примерно по такому же принципу работает DDoS-атака.

Для чего же используются DDoS-атаки? Существует три наиболее распространенных цели совершения данного преступления.

Во-первых, это воздействие на веб-сервер конкурентов. Для того, что парализовать работу компании, бизнес которой напрямую зависит от работоспособности её веб-сайта, конкуренты часто используют DDoS-атаки, в результате чего эти компании терпят огромные убытки в виде упущенной выгоды. Так, около года назад на веб-сервер одной компании по производству и продаже серверов в Санкт-Петербурге была произведена мощная DDoS-атака их конкурентами. Обычная нагрузка веб-сервера данной компании составляет 2-5 запросов в секунду. Во время атаки, которая длилась целые сутки, количество запросов в секунду составляло 6000-7000 запросов, в результате чего сервер перестал функционировать. По подсчетам руководителя отдела по

экономической безопасности упущенная выгода составила 1-1,5 миллиона рублей[48].

Во-вторых, киберпреступники часто совершают DDoS-атаки с целью последующего вымогательства. То есть, они начинают атаковать веб-сервер, затем связываются с его администратором и требуют денежное вознаграждение за прекращение атаки.

В-третьих, существует масса примеров DDoS-атак, совершенных с целью разжигания национальной вражды или с экстремистскими или политическими мотивами. Так, в 2013-2014 годах в связи с непростой политической обстановкой был осуществлен ряд успешных DDoS-атак на сайты Центробанка, ВГТРК, Первого канала, Российской Газеты, МИДа, Межпарламентской ассамблеи ООН, Верховного Совета Крыма и НАТО. Ответственность за данные атаки на себя брали разные DDoS-группировки, как из Украины, так и из России. Многие авторы отмечают, что трансформация киберпреступности в преступность, обладающую политическим характером, представляет собой большую опасность, поскольку становится напрямую связанной с усилением в киберпространстве РФ деятельности представителей хакерский движений, различных спецслужб и силовых структур из зарубежных стран, международных организаций экстремистского характера и террористического толка[49].

Соотношение ст. 272 и ст. 273 УК РФ и определение верной квалификации для DDoS-атаки

Вопросом, который интересует нас с точки зрения уголовного права, является вопрос о том, каким образом квалифицировать данные деяния и являются ли они преступлениями в принципе. Если анализировать DDoS-атаки на предмет наличия общественной опасности в данном деянии, то ответ кажется достаточно очевидным. Каждая из трех вариантов DDoS-атак с точки зрения их

[48] Сведения получены из интервью с руководителем отдела продаж ООО «Сервер Молл» Нариманзаде Тагиром Натиг оглы

[49] Пучков Д.В. Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательства Российской Федерации. Правовая политика и правовая жизнь. 1/2019. – с. 67

целей обладает существенной общественной опасностью. Любая DDoS-атака не просто блокирует возможность использования какого-либо веб-сервера.

Помимо этого, она модифицирует данные десятков, сотен, а порой и сотен тысяч компьютеров третьих лиц. И кроме того, целью DDoS-атаки будет также воздействие на иной объект, не связанный со сферой компьютерной информации. Такими объектами могут быть либо экономическая деятельность, в частности добросовестная конкуренция, либо такое преступления будет совершено против собственности, либо даже против основ конституционного строя и государственной безопасности.

Если говорить об основном объекте данных преступлений и квалификации преступления по одному или нескольким из составов преступлений главы 28, то необходимо обратить внимание на ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание, использование и распространение вредоносных компьютерных программ) и ст. 274.1 (неправомерное воздействий на критическую информационную инфраструктуру Российской Федерации).

В поисках ответа на вопрос о возможных вариантах уголовно-правовой квалификации таких деяний, нами была проанализировала судебная практика. Всего за период с 2012 года по май 2021 года нами обнаружено лишь четыре уголовных дела в отношении DDoS-атак. Что удивительно, все эти дела датированы 2012-2014 годами. Возможно, это можно объяснить, во-первых, тем, что на сегодняшний день DDoS-атаки совершаются с таким уровнем латентности, что для правоохранительных органов практически не представляется возможным найти источник кибератак. Одной из основных причин такой повышенной латентности является то, что большинство не обращается в органы в таких ситуациях, а просто игнорирует произошедшее. Во-вторых, на данный момент уже созданы механизмы противодействия DDoS-атакам, которые порой бывают довольно эффективными.

Так или иначе, мы полагаем необходимым проанализировать имеющуюся судебную практику по данному вопросу. Что представляется интересным, так

это то, что в четырех аналогичных с точки зрения основного объекта (т.е. компьютерной информации) делах, имеется три варианта возможной квалификации.

Первым вариантом квалификации, представленном в Приговоре Шпаковского районного суда № 1-333/2013 от 17 октября 2013 г. по делу № 1-333/2013, является квалификация совершения DDoS-атаки по **ч. 2 ст. 273 УК РФ,** то есть суд расценил DDoS-атаку как вредоносную компьютерную программу. Что касается фабулы дела, то осужденный по данному делу осуществил DDoS-атаку на веб-ресурс и потребовал денежную сумму за прекращение атаки. Таким образом, в данном случае суд констатировал наличие преступления в виде использования компьютерной информации для несанкционированного блокирования средств защиты компьютерной информации, совершенное из корыстной заинтересованности. Дополнительную статью, предусмотренную за вымогательство, суд не вменил.

Вторым вариантом квалификации, представленном в Апелляционном постановлении Московского городского суда № 10-11502/2013 от 25 ноября 2013 г. по делу № 1-9/13, является квалификация **по ч. 2 ст. 272 УК РФ.** В данном деле речь идет о совершении осужденными аналогичной по отношению к первому делу с технической точки зрения DDoS-атаки, однако на этот раз с целью дискредитации конкурента. Таким образом, в данном случае суд констатировал совершение неправомерного доступа к охраняемой законом компьютерной информации, то есть информации в системе ЭВМ и их сети, повлекшей блокирование и нарушение работы системы ЭВМ и их сети, группой лиц по предварительному сговору. При этом суд также не вменил никаких дополнительных статей в части причинения вреда общественным отношениям, связанным с осуществлением экономической деятельности, как, например, ст. 169 УК РФ или ст. 14.33 КоАП.

Третьим вариантом квалификации, представленном в Приговоре Саянского городского суда № 1-14/2014 от 21 января 2014 г. по делу № 1-14/2014 является квалификация **по совокупности ст. 272 и 273 УК РФ.** В

Приговоре Саянского городского суда осужденный совершал ряд DDoS-атак с целью истребования у потерпевших денежных средств. За каждый эпизод он был приговорен к ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ.

Таким образом, при наличии совершенно аналогичных с технической точки зрения деяний, мы имеем три принципиально взаимоисключающих варианта квалификации. Полагаем, данная проблема имеет место в связи с тем, что, во-первых, речь ведется о крайне специфической преступности, квалификация которой требует не только правовых знаний, но и специальных. Кроме того, как указывалось выше, в нынешнем законодательстве, в доктрине и, как следствие, судебной практике, существует большая путаница с используемыми терминами. То есть, в общем-то, термины «цифровая информация», «электронная информация», «средства защиты компьютерной информации», «несанкционированное блокирование», «неправомерный доступ к компьютерной информации» и т.д. обладают некоей степенью условности, что, в общем, препятствует точной и верной квалификации. Так, не совсем ясно, DDoS-атака, которая включает в себя два этапа: заражение компьютеров третьих лиц и направление искусственных запросов на веб-сайт, является примером неправомерного доступа к компьютерной информации или всё-таки распространением и использованием вредоносной программы?

Мы полагаем, что ответ на данный вопрос кроется в формулировках объекта и объективной стороны каждого из составов преступлений. Так, непосредственным предметом состава преступления ст. 272 является безопасность компьютерной информации, охраняемой законом. Предметом данного преступления является информация, которая, во-первых, должна охраняться законом, а, во-вторых, должна соответствовать определению, данному в УК РФ: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». При этом, как

отмечает большинство авторов[50], судебная практика исходит из понимания информации в широком смысле, то есть в смысле любой информации, сохраненной в электронном виде. Объективной стороной преступления, предусмотренного ст. 272, является неправомерный доступ к компьютерной информации, повлекший наступление одного из альтернативных последствий: уничтожение, блокирование, модификация либо копирование. При этом, разумеется, необходимо установить причинную связь деяния и последствий. Кроме того, перечисленные выше последствия могут влечь и иные последствия, являющиеся причиной вменения квалифицированных составов. При этом понятия неправомерности доступа и охраняемости информации основываются на том, что информация не находится в открытом доступе, то есть субъект преступления не имеет права на получение информации, которую он получает в ходе совершения преступления. Так, исходя из смысла статьи 272 УК РФ и ст. 4 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» защите подлежит только зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, то есть документированная информация. По условиям ее правового режима информация ограниченного доступа подразделяется на: отнесенную к государственной тайне (ст. 2 Федерального закона от 21 июля 1993 г. N 5485-I «О государственной тайне») и конфиденциальную, то есть документированную информацию, доступ к которой ограничивается в соответствии с законодательством РФ (ст. 2 Закона об информации). Режим доступа к конфиденциальной информации может быть установлен как ее собственником, так и непосредственно в соответствии с действующим законодательством. Исчерпывающий перечень к категории сведений конфиденциального характера

[50] Бимбинов А.А., Боженок С.А., Грачева Ю.В., Жевлаков Э.Н., Звечаровский И.Э., Иногамова-Хегай Л.В., Клепицкий И.А., Корнеева А.В., Кочои С.М., Левандовская М.Г., Новикова Е.В., Маликов С.В., Молчанов Д.М., Орешкина Т.Д., Палий В.В., Понятовская Т.Г., Рарог А.И., Рубцова А.С., Соктоев З.Б., Суспицына Т.П., Устинова Т.Д., Цепелев В.Ф., Чучаев А.И., Юрченко И.А. Уголовное право Российской Федерации. Особенная часть (учебник) (под ред. д.ю.н., проф. И.Э. Звечаровского). - М.: "Проспект", 2020. - 688 с.

определены в Указе Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»:

а) персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, - ст. 2 Закона об информации), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

б) сведения, составляющие тайну следствия и судопроизводства;

в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

г) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и иными федеральными законами (врачебная, нотариальная и адвокатская тайны, тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и др.);

д) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и иными федеральными законами (коммерческая тайна);

е) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Относительно такой информации собственником или иным правомочным лицом должны быть приняты меры специальной защиты машинной информации (например, введена система паролей или определенная дисциплина работы с информацией), ограничивающие к ней доступ.

Также данные понятия могут основываться на букве закона. Применительно к анализируемой ситуации нас интересует такое последствие, как модификация. Модификация – это любое изменение программного обеспечения, текстовых файлов, изображений и т.п., искажающее информацию по сравнению с ее первоначальным состоянием.

Что касается ст. 273, то её непосредственным объектом является безопасность компьютерной информации от воздействия вредоносных компьютерных программ. Объективная сторона преступления заключается в совершении одного из трех альтернативных действий: создание программы или иной компьютерной информации, их использование или их распространение. Целевое предназначение таких программ или информации: для несанкционированного уничтожения, блокирования, модификации или копирования компьютерной информации или для нейтрализации средств ее защиты. При этом созданием программы являются действия по ее написанию на определенном языке программирования в формате, пригодном для использования в устройстве, способном к восприятию компьютерной информации. Использованием программы являются действия по реализации основных функциональных особенностей программы в отношении любой без ограничений информации (в отличие от ст. 272 данная информация не обязательно должна быть охраняемой), полномочиями на доступ к которой преступник не обладает. Распространение программы предполагает либо совершение действий по непосредственному внедрению вредоносной программы в чужой компьютер, либо распространение ее любым способом (дарение, продажа, рассылка по почте и т.п.) на любом машинном носителе (лазерный диск, карта памяти и т.п.). Классическим примером совершения преступления, предусмотренного ст. 273, можно считать Приговор Тамбовского районного суда Тамбовской области от 2 июля 2020 года по делу № 1-183/2020. В соответствии с данным приговором, Толмачев В.Ю., имея умысел и осознавая, что использует вредоносную компьютерную программу «SQLi Dumper», предназначенную для несанкционированного уничтожения, блокирования, модификации и копирования компьютерной информации, по месту своего жительства, со своей ПЭВМ через информационно-телекоммуникационную сеть «Интернет» запустил компьютерную программу «SQLi Dumper» и применил механизм ее работы в

отношении Интернет-ресурса с доменным именем «agro-ul.ru», принадлежащего Министерству агропромышленного комплекса и развития сельских территорий. В приговоре нет сведений, какие последствия были у использования данной вредоносной программы, однако, исходя из того, что квалификации по совокупности судом назначено не было, следует вывод, что последствия не являли собой другого преступления. При этом, с учетом специфичности области знаний, исходя из судебной практики, вывод об относимости программы к вредоносной во всех случаях должен быть подкреплен экспертным заключением. Кроме того, важно отметить, что данный состав является формальным и не требует наступления общественно-опасных последствий для вменения. Таким образом, преступление считается оконченным с момента совершения любого из возможных действий, указанных в данной статье.

Таким образом, мы сразу видим несколько существенных различий и нюансов. Во-первых, это принципиальная разница в предмете преступления. Так, предметом состава ст. 272 является охраняемая законом компьютерная информация, в то время как предметом ст. 273 является любая компьютерная информация. Данное различие предопределяет необходимость квалификации воздействия вредоносной программы на охраняемую информацию по совокупности статей 272 и 273. Тем не менее, в Приговоре Саянского городского суда № 1-14/2014 от 21 января 2014 г. по делу № 1-14/2014, в котором суд вменил осужденному как ст. 272, так и ст. 273, не указано, что вменение статей по совокупности обусловлено именно разницей в предмете преступлений. Неожиданно, но, суд исходил из логики о том, что деяние осужденного в части ст. 272 повлекло блокирование компьютерной информации, поскольку пользователи сети не могли получить доступ к перегруженному сайту, а значит, данная информация была заблокирована для других пользователей. На первый взгляд может показаться, что такая квалификация неверна, поскольку ст. 272 и 273 не дублируют друг друга, не пересекаются и могут образовать идеальную совокупность лишь в случае

совершения объективной стороны ст. 273 в отношения охраняемой законом информации. Однако, для правильной квалификации необходимо учесть то обстоятельство, что состав ст. 273 является формальным. И тут встаёт главный вопрос. Насколько темпорально разорваны могут быть между собой создание, использование и распространение вредоносной программы? Ведь программа может попадать на ЭВМ третьих лиц в течение нескольких месяцев, а её использование может произойти ещё позже. С какого момента с учетом альтернативности объективной стороны преступление будет оконченным? Ответив на этот вопрос, можно понять сколько раз должна быть вменена ст. 273 и в отношении какой части преступления может быть дополнительно вменена ст. 272. Мы полагаем, что вариант обоснования предложенной квалификации судом является крайне интересным, но довольно сомнительным. Несмотря на то, что для пользователей сайт был заблокирован, неправомерного доступа на ЭВМ пользователей и на сервер «потерпевшего» не осуществлялось, ведь зайти на сайт, в каком угодно количестве пользователей, - это вне всяких сомнений нельзя считать неправомерным доступом. Поэтому в данной ситуации не имеет смысла оценивать информацию как охраняемую или нет, поскольку во время атаки ботов неправомерный доступ не осуществляется, так как переход на сайт – это совершенно правомерное действие. Соответственно, вопрос состоит лишь в том, сколько раз должна быть вменена ст. 273 и сколько оконченных преступлений, предусмотренных ст. 273, будет совершено. Саянский городской суд квалифицировал каждый акт DDoS-атаки, совершенный осужденным, отдельно по ст. 272. Как указано выше, мы не согласны с такой квалификацией. Исходя из данных приговора, всего осужденным было совершено три атаки, первая из которых произошла через несколько месяцев после того, как осужденный приобрел и модифицировал вредоносную программу для создания ботов. Если не ориентироваться на вмененную статью, то необходимо отметить, что суд пошёл по пути оценки каждого акта (создание программы и три акта использования) как отдельного уголовно-правового эпизода. Нам представляется верным такой подход, даже несмотря на общее правило о том,

что альтернативная диспозиция не требует вменения по совокупности. Критерием для принятия решения о квалификации по совокупности, как и в других составах с альтернативной объективной стороной, должно являться единства умысла. В анализируемом приговоре осужденный сначала создал и подготовил к использованию вредоносную программу. Спустя несколько месяцев он разместил объявление о том, что может «организовать» DDoS-атаку. Спустя ещё около месяца ему поступил первый «заказ». И последующие два эпизода происходили с разрывом в несколько месяцев, по вновь возникшим заказам, незапланированно, заказчиками были разные лица, оплата происходила за каждую атаку отдельно. Соответственно, можно сделать вывод о том, что каждый совершенный осужденным эпизод охватывался отдельным умыслом, что позволяет квалифицировать данные преступления по совокупности. При этом, если бы осужденным была подготовлена вредоносная программа для конкретной атаки, то мы полагаем, что данное деяние должно было бы быть квалифицировано по ст. 273, вмененной единожды. Таким образом, мы полагаем, что ст. 272 и 273 не пересекаются в своей объективной стороне и принципиально различаются предметом. Поэтому квалификация по совокупности может иметь место только в том случае, когда воздействие вредоносной программы и неправомерный доступ были совершены в отношении охраняемой законом информации.

2.2.2. Проблема многообъектности и квалификации по совокупности со ст. 163, ст. 167 УК РФ.

Еще одной проблемой DDoS-атак является проблема многообъектности данных преступлений. Например, говоря о случаях DDoS-атак с целью последующего истребования денежных средств у администраторов веб-сайтов, неясно, имеется ли в данном случае также состав преступления, предусмотренного ст. 163, а именно вымогательства. Известно, что признаками вымогательства являются требование совершения действий имущественного характера (в данном случае передачи денежных средств), а также наличие либо угрозы применения насилия (в данном случае это неактуально), либо угрозы

уничтожения или повреждения чужого имущества. Таким образом, для ответа на вопрос о возможности квалификации данного деяния по совокупности статей главы 28 и ст. 163 УК РФ необходимо понять, можно ли считать веб-сайт имуществом, ведь именно ему причиняется вред? С точки зрения гражданского права и домен, и веб-сайт можно считать имуществом. Однако термин «имущество» имеет другое значение для уголовно-правовой отрасли. И для уголовного права имущество – это вещи, деньги, ценные бумаги и другие предметы материального мира, обладающие стоимостью. То есть, если ориентироваться такое, на наш взгляд, достаточно анахронизмичное определение имущества, то действия киберпреступника по истребованию денежных средств по сути являются законными, что кажется достаточно неоднозначным. Проблемы стремительно устаревющего законодательства в сравнении с динамично развивающейся реальностью применительно к проблемам квалификации преступлений в сфере компьютерной информации отмечают многие авторы. Так, Д.В. Пучков говорит о том, что к основным проблемам таким преступления необходимо отнести несоответствие действующего российского уголовного законодательства, в котором отсутствует прогностичность регламентации ответственности за совершение киберпреступлений при наличии достаточно быстро устаревающего официального закрепления и той ограниченной группы деяний, использующих термин «компьютерная информация»[51]. Тем не менее, если следовать формально букве закона, то действия преступников в части истребования денежных средств не подлежат уголовно-правовой квалификации. Каким бы неожиданным это ни казалось, данный вывод подтверждает и имеющаяся судебная практика. Тем не менее, в литературе нам удалось найти информацию, в соответствии с которой аналогичные действия предлагалось квалифицировать по совокупности. Так, в 2003 г. программисты И. Максаков, А. Петров и Д. Степанов в течение полугода организовывали DDoS-атаки на серверы

[51] Пучков Д.В. Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательства Российской Федерации. Правовая политика и правовая жизнь. 1/2019. – с. 69

британских букмекерских контор. Нападения производились с тем расчетом, чтобы букмекеры несли максимальные потери. За прекращение вмешательства программисты требовали с владельцев компаний выкуп в размере 10—20 тыс. долл. По данному факту было возбуждено уголовное дело по ст. 163 и ст. 273 УК РФ[52]. Однако, разумеется, на сегодняшний день такое решения нельзя считать законным, особенно, учитывая принцип толкования всех сомнений в пользу обвиняемого. В то же время с материально-правовой точки зрения нам такая ситуация видится некорректной и устаревшей, особенно в связи с тем, что никаких составов, альтернативных вымогательству и «перекрывающих» данное деяние, не имеется. Для решения данной квалификационной проблемы мы усматриваем два варианта редакций в УК РФ. Во-первых, возможно расширить понятие «имущества» в уголовном праве путём включения в него ряда нематериальных (не осязаемых физически объектов) и приблизить его формулировку к понятию имущества в гражданском праве. В данной ситуации существует риск того, что разновидности имущества с течением времени будут лишь расти, а значит, полное расширение границ понятия может быть чревато включением в него каких-то неоднозначных для уголовно-правовой охраны объектов типа криптовалюты. Кроме того, такая редакция позволит вменять по совокупности в том числе ст. 167 ко всем случаям преступлений в сфере компьютерной информации, ведь так или иначе определенный вред наносится данным нематериальным объектам. Также неясно, как будет устанавливаться размер нанесенного ущерба. Таким образом, такое решения на сегодняшний день является спорным. Во-вторых, существует вариант включения в статьи главы 28 квалифицирующего признака о выдвижении имущественных требований передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой продолжения совершения действия, предусмотренного ч. 1 каждой статьи. Такое регулирование будет

[52] Стенин А. Русские хакеры обокрали англичан // Российская газета. 2004. 29 июля

более «безопасным», поскольку не повлечет глобальных изменений в понимании имущества для всего уголовного права, однако сделает главы 28 более гибкой для крайне частых ситуаций вымогательства денежных средств киберпреступниками.

Ещё одним спорным вопросом является возможность привлечения лиц, совершивших DDoS-атаку к уголовной ответственности по ст. 167 за умышленное повреждение имущества. Так, в ходе DDoS-атаки полностью блокируется весь функционал сервера, который и является в данном случае имуществом, о котором идет речь. Ведь сервер – это физически осязаемая ЭВМ, предмет материального мира, находящийся в чьей-то собственности. Но тут не ясно, можно ли считать блокировку его функционирования его повреждением, так как не ясно, термин «повреждение» в диспозиции ст. 167 подразумевает именно физическую «поломку» или программную в том числе? В любом случае, поскольку сервер становится в момент атаки непригодным к использованию, вопрос об умышленном повреждении имущества встаёт особенно остро Тем не менее, мы полагаем, что такая квалификация будет неверной по следующим обстоятельствам. Блокировка функций сервера не меняет его реальной стоимости. То есть, разумеется, в момент атаки сервер является непригодным к использованию и налицо повреждение информационного, программного характера, однако, на самом деле своих товарных качеств он не теряет и не меняет. Таким образом, при DDoS-атаке нет посягательства на отношения собственности. Соответственно, мы считаем невозможным квалификацию такого деяния по ст. 167, что также подтверждается судебной практикой.

Что касается DDoS-атак по политическим мотивам, то в судебной практике нет ни одного подобного дела по той причине, что с точки зрения уголовно-процессуальной найти такого киберпреступника крайне сложно, хотя в прессе и литературе имеется информация об их совершении, поэтому вопросы квалификации таких деяний ещё более неоднозначны.

2.3. Проблемы квалификации преступлений в сфере компьютерной информации по совокупности с иными преступлениями

Поскольку, как указывалось выше, преступления в сфере компьютерной информации зачастую выступают способом достижений иных преступных целей и имеют так называемый «инструментальный» характер[53], встаёт вопрос о необходимости квалификации преступлений в сфере компьютерной информации по совокупности с иными преступными деяниями.

2.3.1. Квалификация по совокупности со ст. 138, ст. 183, ст. 283.1 УК РФ

Так, необходимо сказать о проблеме уголовно-правовой оценки посягательств на охраняемую законом информацию в случае совершения такого преступления путём доступа к компьютерной информации. Понятие охраняемой законом информации приводилось выше, но в качестве примера можно привести личную, семейную, банковскую или государственную тайны. Так, большим вопросом является ситуация, если преступным деянием нанесен вред не только компьютерной информации, но и личной/коммерческой/государственной тайне, то являет ли такого рода преступление собой идеальную совокупность и должно ли оно квалифицироваться по ст. 272 и по ст. 138 УК РФ, 283.1 УК РФ, 183 УК РФ? Ориентируясь на общую канву законодателя и правоприменителя о том, что деяния, предусмотренные главой 28, не являются квалифицирующими признаками, а являются самостоятельными составами с отдельными объектами, а также с учётом рекомендаций Верховного Суда РФ относительно квалификации по совокупности со ст. 159.6, то кажется вполне логичным квалификация по совокупности. К такому же выводу приходят суды в своем большинстве. Так, например, Приговором Тайшетского городского суда Иркутской области от 10 июня 2014 г. по делу N 1-211/2014 осужденный, который при помощи персонального компьютера, используя полученные путём

[53] Д.А. Мелешко, Д.О. Черняевский, Г.А. Шарафетдинова. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию. Журнал «Законность» № 3, март 2020 г. с. 55

обмана у потерпевшей её логин и пароль от персональной страницы в социальной сети «ВКонтакте», осуществил доступ к хранящейся на ней компьютерной информации, а именно личной переписке потерпевшей с другими пользователями, и при помощи компьютерной программы сделал скриншоты её личной переписки, тем самым скопировал компьютерную информацию к себе на персональный компьютер, был приговорен к ч. 1 ст. 272 и ч. 1 ст. 138 УК РФ. Также в Приговоре Чертановского районного суда г. Москвы № 1-618/2017 по делу 15 декабря 2017 речь идет о том, что осужденная с использованием своего служебного положения неправомерно передала в распоряжение третьему лице абонентский телефонный номер, обеспечив ему доступ к личной переписке, фотографиям, телефонным переговорам и т.д. Суд вменил осужденной совокупность по ч. 3 ст. 272 и ч. 2 ст. 138. Аналогичные решения имеют место в отношении коммерческой тайны. Так, осужденный, являясь работником ООО "М", не имел доступа к коммерческой тайне. Вместе с тем, используя логин и пароль третьего лица, действуя со своего персонального компьютера, получил доступ к сведениям, составляющим коммерческую тайну, после чего совершил копирование указанной информации на внешний накопитель. По приговору Канавинского районного суда г. Нижний Новгород от 6 июня 2018 г. по делу N 1-283/2018. осужденный признан виновным в совершении преступлений, предусмотренных ст. 272 и 183 УК РФ.

Тем не менее, для проверки данного мнения, необходимо ответить на вопросы о том, может ли ст. 272 поглощать ст. 138, и как соотносятся данные составы преступлений. Так, объектом преступления, предусмотренного ст. 138 являются общественные отношения, обеспечивающие реализацию права на тайну переписки, телефонных переговоров и сообщений граждан. То есть такое преступление предполагает преступное воздействие именно на охраняемую законом тайну. При этом объектом ст. 272 УК РФ является безопасность компьютерной информации, охраняемой законом. Соответственно, необходимо понять, как соотносятся понятия «тайна» и «информация,

охраняемая законом». Что касается охраняемой законом информации, то, как указывалось выше, мы снова упираемся в перечисление разновидностей информации особого режима с ограниченным доступом и к перечню такой информации, определенному в Указе Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера». Получается, что при попытке раскрыть понятие «охраняемой законом информации» мы приходим к тем самым «тайнам», которые являются непосредственными объектами статей 183, 138, 283.1. К такому же выводу относительно раскрытия понятия «охраняемой законом информации» для главы 28 УК РФ приводит Верховный Суд Республики Крым в своей Справке по результатам изучения судебной практики по уголовным делам о преступлениях в сфере компьютерной информации (глава 28 УК РФ). Получается, что по сути объект ст. 272 полностью раскрывается через объект смежных преступлений. Таким образом, мы полагаем, что поскольку объект ст. 272 полностью включает в себя объект ст.ст. 138, 183, 283.1, квалификация по совокупности не требуется, поскольку будет противоречить принципу недопустимости двойного вменения. На самом деле даже авторы, защищающие обратную позицию, косвенно подтверждают её уязвимость. Например, Д.А. Мелешко, Д.О. Черняевский, Г.А. Шарафетдинова утверждают, что в такой ситуации необходима квалификация по совокупности. Однако, ниже в своем исследовании они анализируют ситуацию, при которой осужденный, используя принадлежащий ему ноутбук, имеющий доступ к сети Интернет, осуществил поиск и копирование вредоносной компьютерной программы, заведомо предназначенной для перебора учётных данных пользователей торговой площадки "ebay.com" и получения полного доступа к аккаунтам третьих лиц. После этого он осуществил запуск указанной вредоносной программы и в результате её использования получил аутентификационные данные (логин, пароль), а также иные персональные данные 69 граждан Венгрии, Великобритании, США, Франции, Индии, Бельгии, Италии, Бразилии, Швейцарии, Австралии, Швеции, Гваделупы, Китая, являющихся

пользователям интернет-ресурса "ebay.com". При этом органами предварительного расследования и судом действия А. были квалифицированы по ч. 1 ст. 273 УК РФ54. Тогда авторы утверждают, что квалификация неверна и выдвигают версию о том, что верной квалификацией будет квалификация по совокупности ст. 272 и 273, однако, они не указывают, что в данной ситуации крайне вероятно квалификация по ст. 138 с учетом того, что осужденный получил доступ к личным аккаунтам данных лиц и другим персональным данным. Напротив, высказанная нами позиция подтверждается многочисленными судебными решениями. Так, Железнодорожный районный суд г. Хабаровска в приговоре № 1-291/2020 от 10 июля 2020 года по делу № 1-29/2020 признал осужденного виновным в совершении неправомерного доступа к охраняемой законом компьютерной нформации, что повлекло копирование компьютерной информации с использованием своего служебного преступления. Осужденный осуществил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в информационной системе «GreenField», принадлежащей АО «Мегафон Ритейл» и произвел копирование детализации вызовов абонентского номера, зарегистрированного и находящего в пользовании у третьего лица, путем печати на бумажный носитель без поступления в АО «Мегафон Ритейл» согласия указанного абонента. Таким образом, несмотря на то, что осужденный нарушил тайну телефонных переговоров потерпевшего, суд вменил ему лишь ч. 3 ст. 272 УК РФ. Существует также иные судебные решения, подкрепляющие данную позицию[55].

2.3.2. Квалификация по совокупности со ст. 128.1 УК РФ

Следующим вопросом квалификации по совокупности является вопрос о ст. 128.1 УК РФ, предусмотренной за клевету. Так, одним из последствий неправомерного доступа к компьютерной информации может являться

54 Приговор Северского городского суда Тамбовской области от 17 мая 2018 г. по делу N 1-135/2018.

55 Приговор Яйского районного суда Кемеровской области от 21 мая 2018 г. по делу N 1-46/2018; Приговор Автозаводского районного суда г. Тольятти Самарской области № 1-426/2020 от 18 мая 2020 г. по делу № 1-426/2020

распространение в сети Интернет заведомо ложных сведений, порочащих честь и достоинство потерпевшего или подрывающих его репутацию. Объектом данного преступления выступают честь и достоинство личности. Таким образом, очевидно, что «сфера действия» данного состава не пересекается со «сферой действия» ст. 272. Соответственно, в такой ситуации очевидно необходима квалификация по совокупности. К такому же выводу приходят авторы статей[56] и суды. Например, осужденная совершила неправомерный доступ к принадлежащему потерпевшему электронному почтовому ящик. Кроме того, она внесла заведомо ложные сведения о том, что потерпевшая оказывает услуги сексуального характера за денежное вознаграждение, а также распространила на её странице фотографии, доступные для неограниченного числа пользователей. При этом осужденная достоверно знала, что сведения носят заведомо ложный характер и порочат честь и достоинство К. Постановлением Завьяловского районного суда Удмуртской Республики от 1 августа 2011 г. действия виновной были квалифицированы по ч. 1 ст. 128.1 и ч. 2 ст. 272 УК РФ.

2.3.3. Квалификация преступлений с использованием служебного положения

Как отмечают многие авторы, из общего правила квалификации по совокупности есть ещё одно общепризнанное исключение. Таким исключением являются случаи, когда состав компьютерного преступления охватывает состав преступления, выступающего результатом преступных действий, а именно случаи совершения компьютерных преступлений с использованием служебного положения. Как отмечают многие авторы[57], в такой ситуации необходимо ориентироваться на правило квалификации о том, что квалификация составного преступления производится по одной статье в тех

56 Евдокимов К.Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела. - Российский следователь, 2017, N 4, с. 39-44

57 Д.А. Мелешко, Д.О. Черняевский, Г.А. Шарафетдинова. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию. Журнал «Законность» № 3, март 2020 г. с. 56

случаях, когда санкция за такое преступление является более строгой по сравнению с санкцией нормы-части. То есть, если санкция за компьютерное преступление, совершённое с использованием служебного положения, более строгая, чем санкция за служебное преступление, то применению подлежит лишь норма о компьютерном преступлении. Например, совершение должностным лицом из личной заинтересованности незаконных действий, связанных с неправомерным доступом к информации, содержащейся в служебной базе данных, повлёкших её изменение, охватывается ч. 3 ст. 272 УК и не требует квалификации по ч. 1 ст. 285 УК. Если же служебное преступление имеет равную или более строгую санкцию по сравнению с компьютерным преступлением, то конкуренции уголовно-правовых норм нет и содеянное образует совокупность преступлений58.

2.3.4. Совокупность ст. 272 и ст. 273 на примере несанкционированного подключения и просмотра спутниковых каналов

Как отмечалось выше, ещё одной особенностью компьютерных преступлений является то, что для самих составов главы 28 между собой характерна идеальная совокупность. Например, зачастую создание/распространение/использование вредоносных программ часто используется для дальнейшего получения несанкционированного доступа к компьютерной информации. Такой группой дел являются дела, связанные с несанкционированным подключением и просмотром спутниковых каналов. Например, в одном из дел осужденный использовал подключение к сети Интернет и установил на купленный им заранее ТВ_Тюнер измененное программное обеспечение, содержащее вредоносную программу. С использованием данной программы возможен был просмотр платных спутниковых каналов путём копирования компьютерной информации и её передачи через Интернет без ведома законного владельца. Осужденный

58 Проблемы квалификации преступлений: Монография / Под ред. К.В. Ображиева, Н.И. Пикурова. М., 2019, с. 252.

пользовался данной схемой и просматривал каналы бесплатно, получив к ним доступ незаконно с помощью вредоносной программы. Приговором Ленинского районного суда г. Махачкалы от 23 октября 2017 г. по делу N 1-423/2017 он был признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 2 ст. 273 УК РФ. Схожую ситуацию отражает Приговор Собинского городского суда Владимирской области № 1-1-120/2020 от 29 мая 2020 г. В соответствии с фабулой дела осужденный приобрел ресивер и использовал его со смарт-картой для обеспечения незаконного доступа к просмотру платных спутниковых телеканалов. Так, на указанной карте содержалась компьютерная информация (измененные сведения о подписках и сроках их действия), позволяющая осуществлять несанкционированный доступ к информации, содержащейся в системах ЭВМ системы спутникового телевидения, а сама карта при ее использовании, вопреки блокировке и прекращению оказания услуг провайдером, позволяла декодировать защищенные спутниковые телеканалы и получать доступ к просмотру защищенных спутниковых телеканалов. Таким образом, осужденный использовал компьютерную информацию, содержащуюся на смарт – карте, заведомо предназначенную для несанкционированной модификации, копирования и нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности. Суд вменил осужденному ч. 2 ст. 272 и ч. 2 ст. 273. По сути к аналогичным выводом приходит Верховный Суд Республики Марий Эл в апелляционном постановлении № 22-548/2020 от 15 июля 2020 года.

2.3.5. Дела об уничтожении информации

В ходе анализа правоприменительной практики нами также была выявлена ещё одна категория дел – это дела, в которых шла речь об уничтожении информации. Так, в соответствии с кассационным определением Верховного Суда РФ от 13 августа 2008 года № 89-О08-49 Слепчуков Д.А., выполняя указания Важенина С.А., уничтожил информацию об административных правонарушениях шести лиц. Слепчуков Д.А. являлся

администратором автоматизированной информационно-поисковой системы (АИПС), как инженер-программист отдела УГИБДД и был наделен высшим уровнем доступа в сеть, что предоставляло ему права оператора, просмотра, изменения и удаления информации по всем АИПС. То есть, Важенин С.А., являясь сотрудником ГИБДД, в период с декабря 2004 года по август 2005 года получил от шести физических лиц денежные средства (все шесть эпизодов были признаны реальной совокупностью по п. а ч. 4 ст. 290 УК РФ), пообещав уничтожить имеющуюся информацию о совершении ими административных правонарушений, после чего давал указания Слепчукову Д.А. об уничтожении данной информации из АИПС. Приговоров Тюменского областного суда от 17 марта 2008 года Слепчуков Д.А. был признан виновным в совершении шести преступлений, предусмотренных ч. 1 ст. 272 УК РФ, а Верховный Суд РФ оставил данный приговор без изменений. Аналогичная с правовой точки зрения ситуация имела место в Приговоре Фокинского районного суда г. Брянска Брянской области от 29 апреля 2020 года по делу № 1-120/2020. В соответствии с данным приговором Гаврилюк О.В., действуя умышленно, на почве личных неприязненных отношений к сотрудникам организации, в которой она работала, возникших в связи с ее увольнением оттуда, посредством своего ноутбука, используя ранее ей известные в связи с исполнением служебных обязанностей в данной организации логин и пароль от его электронного почтового ящика, осуществила неправомерный доступ к охраняемой законом компьютерной информации – сведениям (сообщениям), находящимся в данном электронном почтовом ящике, в процессе чего модифицировала компьютерную информацию, заменив указанные при регистрации этого ящика абонентские номера на принадлежащий ей абонентский номер, а также уничтожила компьютерную информацию, удалив 187 электронных писем, находившихся в указанном ящике. Вследствие совершения данного деяния Гаврилюк О.В. была признана виновной в совершении ч. 1 ст. 272 УК РФ. Таким образом, в данной группе дел имеется единообразие практики и общий подход к квалификации такого рода преступлений.

Заключение

В ходе проведенной работы мы проанализировали ряд доктринальных и практических квалификационных проблем, связанных с преступлениями в сфере компьютерной информации.

Так, в результате изучения различных позиций авторов, нам удалось предложить варианты определений родового объекта как отношений общественной безопасности и общественного порядка в целом, включающие в себя общественную безопасность, здоровье населения и общественную нравственность, экологическую безопасность, безопасность движения и эксплуатации транспорта, видового объекта как группы общественных отношений, в которые включены права и интересы субъектов, по обеспечению безопасности использования информации и информационных ресурсов, необходимые для нормальной жизнедеятельности общества. Также мы, согласившись с другими авторами, пришли к выводу о том, что непосредственным объектом выступают конкретные общественные отношения, которым преступление причиняет вред или создает угрозу его причинения. Также мы попытались подробно раскрыть понятие предмета преступлений в сфере компьютерной информации, а именно компьютерной информации. Говоря об объективной стороне данного рода преступлений, мы отметили сложности определения места и времени совершения преступлений в связи с тем, что для преступлений в сфере компьютерной информации характера несовпадение места наступления последствий и место совершения преступления, а также зачастую общественно опасные последствия наступают отсроченно.

Также мы затронули вопрос разграничения преступлений в сфере компьютерной информации и мошенничества в сфере компьютерной информации. Нам удалось прийти к выводу о том, что в связи с тем, что ст. 159.6 и преступления главы 28 не соотносятся как часть и целое, поскольку признак «сфера компьютерной информации» в данных составах выполняет разную функцию: для ст. 159.6 функцию средства совершения преступления, а

в главе 28 – объекта, ничто не препятствует квалификации по совокупности. Тем не менее, мы полагаем, что данное юридико-техническое решение несовершенно, поскольку делает состав ст. 159.6 несамостоятельным и невозможным вменению без соответствующей статьи из главы 28. Для решения данного вопроса нами предложено два варианта: исключение ст. 159.6 и внесение соответствующего квалифицирующего признака в ст. 159, либо придание ст. 159.6 черт состава, специального по отношению к составам главы 28.

Кроме того, нами был проанализирован ряд квалификационных проблем не примере DDoS-атак. Поскольку правоприменительная практика по данному вопросу крайне малочисленна и очень разнообразна в своих выводах, нами было предпринято решение о необходимости глубокого анализа сходств и различий составов ст. 272 и 273 для понимания того, какой состав подлежит вменению в такой ситуации. Так, нам удалось прийти к выводу о том, что ключевым различием между ст. 272 и ст. 273 (помимо объективной стороны, разумеется) является предмет преступления, поскольку для ст. 272 предметом является охраняемая законом информация, а для ст. 273 – предмет шире и им является любая информация в целом. Также нам удалось затронуть проблему применения формальных составов с альтернативной объективной стороной, каким и является состав ст. 273. Основываясь на различиях составов ст. 272 и 273 нами был предложены варианты квалификаций в различных ситуациях.

Помимо вышеизложенного мы изучили вопрос многообъектности DDoS-атак и возможность совокупного вменения преступлений главы 28 и ст. 163 и 167 в целом. Так, мы рассмотрели проблему устаревшего определения «имущества» для целей уголовно-правовой защиты, поскольку при формальном подходе в случае совершения преступления в сфере компьютерной информации и дальнейшего выдвижения имущественного требования ради прекращения действия вредоносной программы или атаки, состав вымогательства вменен не может быть, ведь на сегодняшний день компьютерная сеть, база данных, веб-сайт не являются имуществом с уголовно-

правовой точки зрения. Нам видится такой подход принципиально устаревшим, поэтому нами предложены варианты редакций нормативно-правовой базы для решения данной проблемы: глобальный (в виде расширения понятия «имущества» для всего уголовного права) и точечный (в виде внесения квалифицирующего признака в главу 28). Также мы пришли к выводу о невозможности вменения по совокупности ст. 167 УК РФ с учетом настоящего значения термина «имущество», поскольку объектам реального мира при кибератакам вред не наносится, и такой подход нам кажется верным.

Далее нами был проведен анализ правоприменительной практики по вопросу применения судами статей о преступлениях в сфере компьютерной информации. Так, с учетом терминологического сходства и соотношения как целого и частого объекта преступления ст. 272 и ст. 138, 183, 283.1, мы пришли к выводу о невозможности квалификации преступлений по совокупности ст. 138, 183, 283.1 и ст. 272. Также мы пришли к выводу о необходимости квалификации по совокупности ст. 272 и ст. 128.1 в случае, если последствием неправомерного доступа к компьютерной информации является распространение в сети Интернет заведомо ложных сведений, порочащих честь и достоинство потерпевшего или подрывающих его репутацию. Кроме того, нами были рассмотрены особенности квалификации нескольких категорий дел: связанных с несанкционированным доступом к компьютерной информации и связанных с уничтожением информации.

В заключение, необходимо сказать, что на сегодняшний день сфера преступлений в компьютерной информации – это живая, постоянно развивающаяся сфера общественных отношений, требующая уголовно-правовой защиты. Очевидно, что изменения в данном вопросе ещё будут, поскольку даже сегодня существуют юридико-технические проблемы, проблемы несоответствия санкций смежных преступлений, проблемы недостаточного понимания правоприменителем объектов смежных составов. Однако, оценивая динамику на протяжении нескольких лет, можно с уверенностью сказать, что суды стараются выравнивать и решать ошибки

законодателя, а законодатель обращает внимание на недостатки формулировок и старается их исправлять. Будем надеяться, что с учётом работы всех сфер государства, совершенствования уголовно-процессуальных способов раскрытия и пресечения такого рода преступлений, в ближайшее время нам удастся поставить эту сферу под контроль и сделать максимально безопасной для законопослушного общества.

Список литературы

1. Уголовный кодекс Российской Федерации
2. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Федеральный закон от 07.07.2003 N 126-ФЗ «О связи».
4. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи».
5. Вехов В.Б. Компьютерное моделирование при расследовании преступлений в сфере компьютерной информации: учебное пособие / В.Б. Вехов, С.А. Ковалев; под ред. д-ра юрид. наук, проф. Б.П. Смагоринского. Волгоград: ВА МВД России, 2014. 77 с.
6. Вехов В.Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. N 4. С. 2-4.
7. Вехов В.Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. N 10. С. 22-24.
8. Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. М.: Академия Следственного комитета Российской Федерации. 2015. N 2. С. 43-46.
9. Вехов В.Б. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами // Вестник Волгоградской академии МВД России. Вып. 1 (20). Волгоград: ВА МВД РФ, 2012. С. 79-82.
10. Евдокимов К.Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела // Российский следователь. - 2017. - N 4.
11. Проблемы квалификации преступлений: Монография / под ред. К.В. Ображиева, Н.И. Пикурова. - Москва, 2019.
12. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Автореф. … дис. канд. юрид. наук. М., 1998, С. 12.

13. Комментарий к Уголовному Кодексу РФ/ Отв. ред. А.В. Наумов. М., 1996, с. 662.
14. Уголовный кодекс РФ: постатейный комментарий/ Под ред. Н.Ф. Кузнецовой и Г.М. Миньковского. М., 1997, с. 581.
15. Российское уголовное право. Особенная часть/ Под ред. В.Н. Кудрявцева и А.В. Наумова. М., 1997. С. 346.
16. Дворецкий М.Ю. Объект преступлений в сфере компьютерной информации: VI Державинские чтения, 2001, с. 25-26.
17. Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств// Журнал прикладных исследований 2020 г. – 54 с.
18. Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин – Москва: Юридическая литература, 1991. – 272 с.
19. Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук; Сарат. юрид. ин-т МВД РФ – Саратов, 2002 г.
20. Копылов В.А. Информационное право: вопросы теории и практики/ В.А. Копылов – Москва: Юристъ, 2003. – 623 с.
21. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации - Исполнительный комитет СНГ.
22. Бегишев И.Р. Цифровая информация: понятие и сущность как предмета преступления по российскому законодательству// Академический юридический журнал – 2011. 0 № 2 (44) с.10.
23. Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание

ученой степени кандидата юридических наук; Нижегородский юридич. Ин-т МВД РФ – Нижний Новгород, 2000.

24. Борисов Т. Хакеры остановили сердце. Преступность в Интернете дошла до физического устранения людей – прямо по проводам// Рос. газ. 2005. 8 февр.
25. Уголовное право России. Части общая и особенная учебник/ отв. ред. А.И. Рарог – Москва, Проспект, 2016. – 494 стр.
26. Бобраков И.А. Уголовное право: учебник/ И.А. Бобраков – Саратов: Вузовское образования, 2018.
27. Лопатина Т.М. Особенности объекта преступлений в сфере компьютерной информации: Бизнес в законе 1-2`2006, с. 171.
28. Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации. / Пробелы в российском законодательстве – 4`2015, с. 209.
29. Бимбинов А.А., Боженок С.А., Грачева Ю.В., Жевлаков Э.Н., Звечаровский И.Э., Иногамова-Хегай Л.В., Клепицкий И.А., Корнеева А.В., Кочои С.М., Левандовская М.Г., Новикова Е.В., Маликов С.В., Молчанов Д.М., Орешкина Т.Д., Палий В.В., Понятовская Т.Г., Рарог А.И., Рубцова А.С., Соктоев З.Б., Суспицына Т.П., Устинова Т.Д., Цепелев В.Ф., Чучаев А.И., Юрченко И.А. Уголовное право Российской Федерации. Особенная часть (учебник) (под ред. д.ю.н., проф. И.Э. Звечаровского). - М.: "Проспект", 2020. - 688 с.
30. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. - № 10. – С. 25.
31. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 1997. - № 1 – С. 9; Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность // Юридический мир. – 1998. - № 2. С. 350-352; Лопатина Т.М. Особенности объекта преступлений в сфере компьютерной информации: Бизнес в законе 1-2`2006, с. 171.
32. Уголовное право. Особенная часть: учебник / под ред. проф. В.Н. Петрашова. М.: Издательство Приор, 1999. С. 364, 430.
33. Кузнецов А.П. Ответственность за преступления в сфере компьютерной информации: учебно-практическое пособие, 2007. С. 127.

34. Кузнецов А.П., Маршакова Н.Н., Паршин С,М. Преступления в сфере компьютерной информации: учебно-практическое пособие. Нижний Новгород, 2007. С. 184.
35. Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского университета. Серия 11: Право. – 1998. - № 4. – С. 21.
36. Метелев А.В., Образцов В.А., Поздняков В.М., Рычкалова Л.А., Селина Е.В., Степаненко Д.А., Табаков А.В., Тушканова О.В., Устинов А.В., Ширев Д.В., Шмонин А.В. Криминалистика: учебник для бакалавров (под ред. д.ю.н., проф. Л.В. Бертовского). - М.: "Проспект", 2018. – 960, 452 с.
37. Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. № 9.
38. Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Уголовное право и процесс. 2020. VI.
39. Бойко С.Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование. М.: Юрлитинформ, 2019. – 198 с.
40. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1. С. 118.
41. Третьяк М.И. Мошенничество как преступление против собственности в современном уголовном праве: курс лекций. М.: Юрлитинформ, 2014 – 198 С.
42. Савельев И.В. Мошенничество в сфере компьютерной информации: потенции квалификационных страданий // Вопросы российской юстиции. Четвертый выпуск. – 447 с.
43. Приговор № 1-588/2018 от 9 ноября 2018 г. по делу № 1-588/2018
44. Пучков Д.В. Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательства Российской Федерации. Правовая политика и правовая жизнь. 1/2019. – с. 67
45. Стенин А. Русские хакеры обокрали англичан // Российская газета. 2004. 29 июля

46. Д.А. Мелешко, Д.О. Черняевский, Г.А. Шарафетдинова. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию. Журнал «Законность» № 3, март 2020 г. с. 55
47. Приговор Северского городского суда Тамбовской области от 17 мая 2018 г. по делу N 1-135/2018.
48. Приговор Яйского районного суда Кемеровской области от 21 мая 2018 г. по делу N 1-46/2018; Приговор Автозаводского районного суда г. Тольятти Самарской области № 1-426/2020 от 18 мая 2020 г. по делу № 1-426/2020
49. Богданова Т.Н. Наказание за преступления в сфере компьютерной информации // Вестник Челябинского государственного университета. 2013. № 17 (308). С. 49.
50. Приговор Шпаковского районного суда № 1-333/2013 от 17 октября 2013 г. по делу № 1-333/2013
51. Приговор Саянского городского суда № 1-14/2014 от 21 января 2014 г. по делу № 1-14/2014
52. Апелляционное постановление Московского городского суда № 10-11502/2013 от 25 ноября 2013 г. по делу № 1-9/13
53. Приговор Тамбовского районного суда Тамбовской области от 2 июля 2020 года по делу № 1-183/2020
54. Приговор Тайшетского городского суда Иркутской области от 10 июня 2014 г. по делу N 1-211/2014
55. Приговор Чертановского районного суда г. Москвы № 1-618/2017 по делу 15 декабря 2017
56. Приговор Канавинского районного суда г. Нижний Новгород от 6 июня 2018 г. по делу N 1-283/2018
57. Определение Верховного Суда РФ от 13 августа 2008 года № 89-О08-49
58. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»
59. Постановление Завьяловского районного суда Удмуртской Республики от 1 августа 2011 г.

60. Апелляционное постановление Верховного Суда Республики Марий Эл № 22-548/2020 от 15 июля 2020 года.
61. В.Н. Синюков. Фундаментальные проблемы юридической науки. Цифровое право и проблемы этапной трансформации российской правовой системы. МГЮА № 9 (154) Сентябрь 2019 года.